PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS AMBIENTAIS E DE TECNOLOGIAS

LUIZ ANTONIO FOSSALUZZA JUNIOR

CRIPTOGRAFIA ÓPTICA MEDIANTE CONTROLE ANALÓGICO DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS: ANÁLISE PARA SINAIS NRZ E DQPSK

CAMPINAS
2012

LUIZ ANTONIO FOSSALUZZA JUNIOR

CRIPTOGRAFIA ÓPTICA MEDIANTE CONTROLE ANALÓGICO DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS: ANÁLISE PARA SINAIS NRZ E DQPSK

Dissertação apresentada ao Centro de Ciências Exatas, Ambientais e de Tecnologias - CEATEC, da Pontifícia Universidade Católica – PUC - Campinas, como requisito parcial à obtenção do título de Mestre em Gerência de Redes de Telecomunicações.

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

PUC-CAMPINAS
2012

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

t621.3827
F751c

Fossaluzza Junior, Luiz Antonio.
Criptografia óptica mediante controle analógico da amplitude e do atraso de fatias espectrais: análise para sinais NRZ e DQPSK / Luiz Antonio Fossaluzza Junior. - Campinas: PUC-Campinas, 2012.
p.

Orientador: Marcelo Luís Francisco Abbade.
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.
Inclui bibliografia.

1. Comunicações óticas. 2. Telecomunicações - Automação. 3. Criptografia. 4. Análise espectral. I. Abbade, Marcelo Luís Francisco. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Título.

22.ed.CDD – t621.3827

LUIZ ANTONIO FOSSALUZZA JUNIOR

CRIPTOGRAFIA ÓPTICA MEDIANTE CONTROLE ANALÓGICO DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS: ANÁLISE PARA SINAIS NRZ E DQPSK

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em gestão de Redes de Telecomunicações.
Área de Concentração: Gestão de Redes e Serviços.
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Dissertação defendida e aprovada em 23 de novembro de 2012 pela Comissão Examinadora constituída dos seguintes professores:

_____
Prof. Dr. Marcelo Luís Francisco Abbade
Orientador da Dissertação e presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

_____
Prof. Dr. Jorge Diego Marconi
Universidade Federal do ABC

_____
Prof. Dr. Eric Alberto de Mello Fagotto
Pontifícia Universidade Católica de Campinas

Aos meus pais, Luiz Antonio e Nelita
A minha esposa, Celia
A minha filha, Giovana

AGRADECIMENTOS

À Deus, que me iluminou durante toda esta caminhada.

Aos meus pais, Luiz Antonio e Nelita, que sempre incentivaram os meus estudos. Me ensinaram as primeiras palavras e me deram os primeiros livros.

À minha esposa, Celia, e minha filha, Giovana, pela paciência, entendimento, companheirismo e compreensão durante esta longa jornada. Sem os vossos apoios, certamente não teria conseguido chegar até aqui.

Ao meu amigo, chefe e companheiro, João Marcos Menon. Grande incentivador desta conquista.

Também agradeço imensamente a outro companheiro e amigo, Rodrigo Frandsen da Silva, com quem dividi muitas dúvidas e angústias durante a jornada laboratorial. E, lembrando do laboratório, à presteza dos colaboradores da PUC, Eduardo Veiga e Juliana Machado, que me auxiliaram nas realizações das simulações. Não menos importante, a colaboração do angolano Carlos Messani, um futuro engenheiro que, certamente, se destacará pelo seu esforço e competência.

Aos professores, pela importância que tiveram na minha vida acadêmica, e, em especial, o Professor Dr. Marcelo Luís Francisco Abbade, orientador deste trabalho e coordenador do curso, sempre com suas mensagens, dicas e observações valiosas que enriqueceram os meus estudos.

À Pontifícia Universidade Católica de Campinas, por propiciar o ambiente, as ferramentas necessárias e a bolsa de estudos para a conclusão deste curso de Mestrado.

Ao CNPq e à FAPESP pelo financiamento parcial deste trabalho, dentro do escopo do Programa Fotonicom.

“A maior prova de insanidade é fazer
as coisas sempre do mesmo jeito e
querer resultados diferentes.”

(Autor Desconhecido)

RESUMO

FOSSALUZZA JUNIOR, Luiz Antonio. **CRIPTOGRAFIA ÓPTICA MEDIANTE CONTROLE ANALÓGICO DA AMPLITUDE E DO ATRASO DE FATIAS ESPECTRAIS: ANÁLISE PARA SINAIS NRZ E DQPSK.** 2012. Dissertação de Conclusão de Curso para o Mestrado em Gerência de Redes de Telecomunicações. Campinas, 2012.

Este trabalho aborda uma técnica para criptografar o sinal óptico em redes ópticas transparentes (*Transparent Optical Network*, TON), de modo a salvaguardar o sigilo e garantir a segurança das informações que são transmitidas através da Rede de Telecomunicações. A técnica avaliada é relativa à camada física do modelo de referência para interconexão de sistemas abertos (*open systems interconnection*, OSI) e consiste em dividir espectralmente um sinal óptico e em aplicar diferentes atenuações e atrasos a cada uma das fatias espectrais consideradas. A seguir essas fatias são multiplexadas e o sinal resultante, que será propagado por uma rede óptica transparente, estará idealmente ininteligível para intrusos que tentem furtá-lo. Nesse ponto é possível avaliar a qualidade da criptografia utilizada, medindo-se na saída do codificador a taxa de erro de bit (*bit error rate*, BER) do sinal criptografado, BER_C. Em princípio, quanto maior BER_C, menor a probabilidade de um intruso decodificar o sinal. Ao chegar ao seu destino, o sinal é recebido no circuito decodificador, que possui a mesma estrutura física do circuito que codificou o sinal original. A aplicação dos fatores de atenuação e atraso neste sinal distorcido é ajustada para a reconstrução do sinal óptico gerado pelo transmissor. Na saída do decodificador, efetua-se a medição da BER do sinal decodificado, BER_D. Idealmente, BER_D deve ser a menor possível. Para avaliação da técnica, simulou-se, com a versão 8.7 do *software* VPITransmissionMaker, da empresa VPIPhotonics Inc, a operação dos dispositivos de criptografia, da propagação e dos elementos de decriptografia do sinal. Todas as simulações consideraram que o fatiamento espectral foi realizado por meio de filtros com perfil ideal. Os resultados indicam que a BER_C pode atingir até 42% e 24%, para sinais codificados com modulação não retorno ao zero com chaveamento on-off (*non return to zero – on-off keying,* NRZ-OOK) e por deslocamento de fase diferencial em quadratura (*differential quadrature phase shift keying,* DQPSK) respectivamente, e que ambos não apresentam erros ($BER_D < 10^{-15}$ para o sinal NRZ-OOK e $BER_D < 10^{-6}$ para a modulação DQPSK) quando decodificados.

Palavras-chave: Criptografia Óptica, Redes Ópticas Transparentes, Fatiamento Espectral.

ABSTRACT

FOSSALUZZA JUNIOR, Luiz Antonio. ***OPTICAL CRYPTOGRAPHY THROUGH ANALOG CONTROL OF AMPLITUDE AND DELAY OF SPECTRAL SLICES: ANALYSIS FOR NRZ AND DQPSK SIGNALS.*** *Completion of Course Work for the Master Graduation Course in Management Telecommunications Networks. Campinas, 2012.*

This work investigates a technique to encrypt the optical signal for Transparent Optical Network, TON, in order to safeguard the confidentiality and guarantee the security of informations that are transmitted through the Telecommunications Network. The technique is assessed on the physical layer of the reference model for open systems interconnection, OSI, and consists of slicing spectrally optical signal and to apply various attenuations and delays to each of the slices spectral considered. These slices are multiplexed and the resulting signal, which will be propagated by an optical network transparent, it will be ideally unintelligible to eavesdropper who try to steals it. At this point is possible to evaluate the quality of the encryption used by measuring the output of the encoder the bit error rate, BER, the encrypted signal, BER_C. In principle, as highest BER_C,it will be lowest the probability of an eavesdropper decode the signal. To get to your destination, the signal is received in the decoder circuit, which has the same physical structure of the circuit which encoded the original signal. The application of the factors of attenuation and delay in this distorted signal is adjusted for the reconstruction of optical signal generated by the transmitter. On the output of decoder, performs the measurement of BER of signal decoded, the BER_D. Ideally, BER_D must be the lowest possible. For technique evaluation, it was simulated, with the version 8.7 of the software VPITransmissionMaker, of company VPIPhotonics Inc, the operation of the devices of cryptography, propagation and the elements of decoded signal. All simulations considered that the spectral slicing was carried out by means of filters with ideal profile. The results indicates that the BER_C may reach up to 42% and 24%, to encrypted signals with modulation on-off Keying non return to zero (NRZ-OOK) and differential quadrature phase shift keying (DQPSK) respectively, and that both are free of errors ($BER_D < 10^{-15}$ for the signal NRZ-OOK and $BER_D < 10^{-6}$ for DQPSK modulation) when decoded.

Key-words: *Optical Cryptography, Transparent Optical Networks, Spectral Slicing.*

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

O sigilo da informação é um dos principais desafios enfrentados atualmente pelas corporações[1], em especial, pelas instituições financeiras e militares. Neste sentido, torna-se indispensável a manutenção da confidencialidade dos dados que são tramitados entre suas unidades, permitindo, por exemplo, que um segredo industrial não esteja disponível para agentes não autorizados, uma vez que isto pode ser considerado o diferencial competitivo de uma companhia (KITAYAMA, 2011; KARTALOPOLOUS, 2009).

Para ilustrar a importância do assunto, destaca-se que nos Estados Unidos da América foi promulgada a Lei Sarbanes-Oxley (*Sarbanes-Oxley Act*, SOX), assinada em 2002 pelo senador democrata Paul Sarbanes e pelo deputado republicano Michael Oxley. A Lei, que ficou muito conhecida após os escândalos da Enron (empresa americana do ramo de energia) em 2001, e que afetou negativamente a reputação da empresa de auditoria independente Arthur Andersen, versa sobre a criação de mecanismos de auditoria e de segurança, inclusive da informação, em empresas que possuem algum tipo de operação financeira que envolve o exterior, e, em especial, o mercado americano. Entenda-se como segurança da informação não só a garantia do sigilo dos dados, mas também a sua acurácia e confidencialidade, quando aplicável. Em um dos seus requisitos, a Lei aplica multas de US$ 1 milhão diários às empresas que não criptografam os dados confidenciais de seus clientes nas transações financeiras (BORGERTH, 2006).

[1] Corporações: o termo e suas derivações, oriundas do latim *corporis* e *actio*, neste trabalho expressa todos os tipos de organizações, governamentais ou de direito privado, e em especial as instituições financeiras, militares e de pesquisa.

Neste mesmo viés, o Centro de Identificação de Roubo de Recursos (*Identity Theft Resource Center*, ITRC) americano indica que em 2008 houve um crescimento de 47% na violação de dados quando comparados ao ano anterior. A gravidade da situação é que apenas 2,4% destes dados roubados possuíam algum tipo de criptografia ou segurança contra invasão de privacidade. Somado a isto, dados apontam que os custos das corporações para evitar a fraude de dados teve um incremento de 346% entre 2005 e 2009, quando era estimado um dispêndio de US$ 1,5 milhão por incidente e, em 2009, estes valores atingiram a significativa marca de US$ 6,7 milhões. Ou seja, torna-se preocupante assuntos que envolvem a garantia de segurança da informação (Em: <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf>. Acesso em: 25 setembro 2012).

Dentro deste ambiente no qual a necessidade da manutenção da segurança da rede é iminente, as instituições financeiras e militares tomam um lugar de destaque, justamente pelo altíssimo grau de proteção que são requeridos pelos dados que trafegam nestas redes corporativas (SHANEMAN, 2004). Diante disto, cada vez mais estas instituições preocupam-se com a segurança da infra-estrutura das redes de comunicação de dados e, como parte integrante destas estruturas, encontramos as Redes de Telecomunicações. A complexidade dos modelos construtivos destas redes, aliada à necessidade que as corporações têm de estabelecer um espelhamento físico e lógico dos seus *datacenters* e de manter este tráfego de informações sob rigoroso controle são aspectos relevantes e que merecem atenção especial. Também é relevante o fato de que, na maioria das vezes, tal infra-estrutura é de propriedade de terceiros, que são os provedores dos serviços de comunicação de dados. Devido ao elevado custo desta infra-estrutura, estes provedores compartilham tais recursos entre os seus clientes e até mesmo com empresas que são concorrentes dentro de um mesmo mercado.

As redes ópticas compõem parte da infra-estrutura fundamental onde estas informações transitam. Com o aumento expressivo do tráfego de dados registrado nos últimos anos, tornou-se indispensável a aplicação de tecnologias que permitissem a utilização mais eficiente do espectro óptico. Neste contexto, destaca-se a tecnologia de multiplexação por divisão comprimento de onda (*Wavelenght Division Multiplexing*, WDM), que permite que uma fibra monomodo seja capaz de transmitir diversos comprimentos de ondas. Isto incrementa consideravelmente a capacidade de transmissão de dados destas redes.

Embora sejam mais seguras que as redes sem-fio (VIEIRA, 2003), as redes ópticas também estão expostas a ações indesejadas e que podem culminar no furto de informações. Nas redes ópticas com roteamento eletrônico, uma sequência de bits é interpretada após a fotodetecção do sinal óptico que chega a um determinado nó da rede. Tal informação é armazenada no *buffer* do roteador até que haja o estabelecimento da conexão à rota de destino da informação. Durante este período de armazenamento temporário da informação, a presença de um *software* malicioso no roteador pode permitir que a informação seja enviada para algum destino diferente do que é desejado pelo transmissor, comprometendo o sigilo da comunicação.

Já nas redes ópticas transparentes (*Transparent Optical Networks*, TONs) os comutadores ópticos que não armazenam as informações a serem transmitidas substituem os roteadores eletrônicos (RAMASWAMI, 2009). Desta forma, a ausência dos roteadores eletrônicos, confere um maior grau de segurança a esse tipo de rede, quando comparada às redes com roteamento eletrônico. No entanto, ainda é possível o desvio do tráfego da rede para algum destino não autorizado.

Em uma abordagem intrusiva, isso pode ser feito com a inserção de um divisor em uma das caixas de emenda óptica da rede. A inserção de um divisor

(*splitter*) óptico, por exemplo, de 10:1 causaria uma degradação potencialmente imperceptível para a operadora de rede. Outra maneira de acesso não autorizado à informação, seria de forma não intrusiva, acoplando-se à rede um dispositivo que emprega uma curvatura acentuada nos *patch cords* de terminação destas redes e que, através das características de refração do sinal óptico, permite a sua fotodetecção (SHANEMAN, 2004). Dispositivos com estas características, chamados acoplador passivo tipo *clip-on* (*clip-on passive optical fiber*), são facilmente encontrados no mercado e possuem custo relativamente baixo (inferior a US$ 1200) (Em: <http://www.go4fiber.com/spec/PFC%201000.pdf>. Acesso em: 22 setembro 2012).

Dentro do contexto de exposição das fragilidades da segurança das redes, é requerido que a tríade da confidencialidade, integridade e disponibilidade da informação esteja presente quando requisitada (KITAYAMA, 2011). A confidencialidade da informação é atingida se ela não estiver disponível ou se ela não for revelada para entidades não autorizadas. A integridade é a garantia de que esta mesma informação não foi alterada ou destruída sem autorização; enquanto a disponibilidade relaciona a acessibilidade e a aplicabilidade desta informação quando requerida por estas entidades. Há diversos mecanismos que são aplicados às redes de informação e que garantem a manutenção desta tríade.

A criptografia da informação é um destes mecanismos (FOK, 2009; TAJAHUERCE, 2000). A palavra criptografia tem origem grega e significa "escrita secreta". Normalmente, ela é introduzida na camada de apresentação do modelo de referência para interconexão de sistemas abertos (*Open Systems Interconnection*, OSI). No entanto, quanto maior for o número de camadas codificando as informações que estão sob suas responsabilidades, mais robusto será o nível de segurança destes dados (TANENBAUM, 2003; HARASAWA, 2011; CORNEJO, 2009). Como exemplo, o uso de redes privadas virtuais (*Virtual Private Network*, VPN) ou a codificação dos pacotes de dados que saem de uma máquina e são endereçados a outra na camada de enlace de dados, quando

combinado com os protocolos de segurança da Internet (*Internet Protocol Security*, IPSec) aplicados à camada de redes, dão maior privacidade informação, tornando-a menos susceptível a espiões indesejáveis (KITAYAMA, 2011).

Apesar de a criptografia aplicada à camada física ainda ser pouco utilizada em redes (KITAYAMA, 2011; TANENBAUM, 2003; SOWAILEM, 2009), a literatura apresenta vários estudos nesta área, por exemplo, em criptografia quântica (SCHUAT, 2002; KITAYAMA, 2011; TANAKA, 2008; LADD, 2010; TOWNSEND, 1998; TANEMBAUM, 2003; ABBADE, 2012). Essa técnica baseia-se principalmente no fato de dois usuários, mesmo sem nunca terem trocado nenhum tipo de mensagem, podem transferir entre si informações invioláveis, pois a técnica da mecânica quântica permite que seja criada uma única chave de criptografia a cada conjunto de informações transmitidas. Estudos mostram a aplicabilidade da técnica em enlaces de até 97 km (TANAKA, 2008), porém ainda é uma tecnologia de custo elevado e de implementação complexa (TANENBAUM, 2003; LADD, 2010).

Outra técnica de codificação de sinais empregada à camada física de redes ópticas é o acesso múltiplo por divisão de código óptico (*Optical Code Division Multiple Access*, OCDMA). A técnica consiste em atribuir a cada conjunto de transmissor e receptor da informação um código único e exclusivo, permitindo que haja a transmissão simultânea de vários pares de usuários, na mesma faixa de frequências (KOSTINSKI, 2008; WANG, 2007; PRUCNAL, 2009; ETEMAD, 2007; YIN, 2007; CONCOTTI, 2008; WU, 2006; LOPES, 2005). Em princípio, a recuperação do sinal só é possível caso o receptor tenha conhecimento da chave de codificação utilizada pelo seu transmissor-par. O OCDMA é uma tecnologia aplicada às redes de acesso e, pontualmente, em redes metropolitanas (YIN, 2007; CINCOTTI, 2008). Em grande parte de suas implementações, o OCDMA provoca o alargamento espectral do sinal codificado (PRUCNAL, 2009; WU, 2006; LOPES, 2005). Observa-se que, embora não seja prejudicial em redes de múltiplo acesso, tal alargamento não seria aconselhável para criptografar sinais em redes

core. Isto se deve ao fato de que estas redes empregam a tecnologia WDM, utilizando equipamentos que limitam a banda dos canais à uma largura fixa, que é o caso dos multiplexadores e demultiplexadores ópticos.

Ainda dentro das técnicas OCDMA, há um estudo teórico na literatura (CORNEJO, 2007; TOCNAYE, 2008) que propõe uma separação das componentes espectrais do sinal óptico, após a passagem deste sinal por uma grade de difração dispersiva. A cada um desses conjuntos espectrais, é aplicada uma codificação de fase de zero ou π. No estudo, são levados em consideração os efeitos não lineares e dispersivos e que tanto influenciam na qualidade e distância de propagação do sinal óptico. Em contrapartida, não é analisada a qualidade do sinal óptico codificado.

Neste trabalho, propõe-se um modelo de criptografia do sinal óptico em redes ópticas totalmente transparentes (*Transparent Optical Networks*, TONs), a ser aplicada na camada física do modelo de referência OSI. O objetivo é garantir que agentes não autorizados, mesmo tendo desviado parte deste sinal onde está sendo transportada a informação, sejam impedidos de interpretá-lo por desconhecerem a chave de codificação da informação.

A técnica consiste na divisão do espectro óptico em diversas fatias, o que chamamos de fatiamento espectral. A partir daí, aplica-se a cada uma destas fatias, atenuações e atrasos aleatórios, que podem ser ajustados analogicamente pelo módulo de criptografia. Desta forma, a recomposição do sinal só seria possível caso o receptor deste sinal conheça os valores de atenuação e atraso que foi aplicado a cada fatia espectral, além, é claro, da largura de banda e da posição espectral de cada componente deste fatiamento.

Desta forma, no melhor de nosso conhecimento, a técnica proposta difere dos outros estudos encontrados na literatura, pois permite o controle analógico e simultâneo dos parâmetros da variação de amplitude e do atraso, que são aplicados a cada fatia espectral, independente do tipo de modulação do sinal. Tal controle é possível através do emprego de equipamentos disponíveis comercialmente, tais como o WaveShaper ® da Finisar, que permite que todos estes parâmetros sejam ajustados em cada uma destas fatias (Em: <http://www.finisar.com/WaveShaper>. Acesso em: 30 julho 2012).

Observa-se que este trabalho está concentrado na avaliação da técnica considerada em termos dos parâmetros físicos que a afetam (atenuação e atraso das fatias espectrais). A avaliação de técnicas para estipular as chaves criptográficas utilizadas, bem como a robustez a possíveis ataques para identificar essas chaves está além do escopo desta dissertação e é deixada para trabalhos futuros.

Este trabalho está organizado da seguinte maneira. O Capítulo 2 apresenta aspectos importantes sobre a segurança em Redes de Telecomunicações, detalhando alguns conceitos de criptografia e a sua aplicação à camada física, necessários ao entendimento deste trabalho. O Capítulo 3 descreve a simulação, dando detalhes do procedimento utilizado para criptografia óptica por fatiamento espectral e do arranjo de simulação, com a técnica utilizada na propagação da TON. Já nos Capítulos 4 e 5, respectivamente, apresentam-se os resultados das simulações e as nossas conclusões e considerações finais.

2. CRIPTOGRAFIA NA CAMADA FÍSICA

As motivações para o desenvolvimento deste trabalho foram apresentadas no Capítulo 1. Foi mostrada a importância da criptografia dos dados nas Redes de Telecomunicações e os principais estudos que estão sendo desenvolvidos visando garantir o sigilo da informação. Por fim, efetuou-se uma breve descrição da técnica de criptografia óptica proposta neste trabalho, que será abordada no próximo capítulo.

A Seção 2.1 deste capítulo apresenta alguns conceitos gerais sobre criptografia. A Seção 2.2 aborda, de maneira mais detalhada, as técnicas de criptografia mais usadas na camada óptica.

2.1. Conceitos de criptografia

A aplicação da criptografia na transmissão de dados, permitindo que, em princípio, somente os detentores autorizados tenham acesso ao conteúdo que é transmitido é uma estratégia muito utilizada. Neste contexto, particularizar a informação, permitindo que ela esteja disponível quando requerido, sem qualquer alteração e somente para os agentes autorizados é o grande desafio enfrentado pelas empresas e, em especial, para os provedores de comunicação.

A palavra criptografia é uma expressão oriunda do grego e significa “escrita secreta”. Os militares desempenharam o papel mais importante para o desenvolvimento desta tecnologia, apesar de outros grupos, tais como os diplomatas, os amantes e as pessoas que necessitam guardar segredos e memórias também terem contribuído para a disseminação da arte (TANENBAUM, 2003).

A Fig. 1 mostra a aplicação do modelo de criptografia para uma cifra de chave simétrica, ou seja, aquela em que a mesma chave é utilizada para codificar e decodificar a informação transmitida. Desta forma, a chave de criptografia, K_C, e decriptografia, K_D, são iguais. Basicamente, uma informação gerada por um texto simples *P* é submetida a uma chave de criptografia K_C. A combinação do texto *P* e da chave criptográfica dá origem ao texto cifrado ou criptografado *C*.

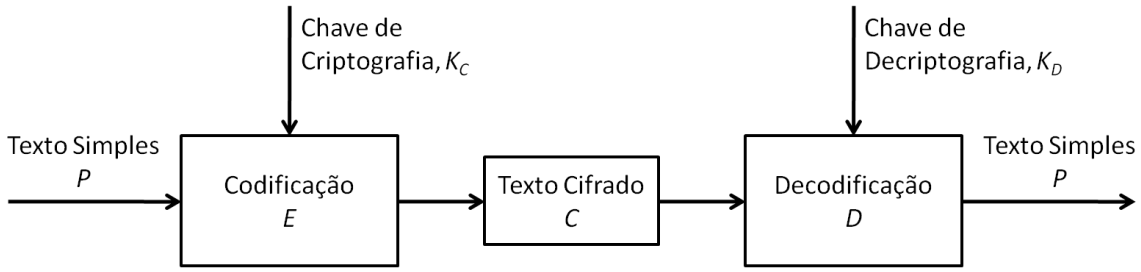


Fig. 1 - Modelo de criptografia para uma cifra de chave simétrica.

Após ser transmitido até o seu destino, a aplicação da chave de decodificação ou decriptografia K_D na informação cifrada *C*, nos permite a recuperação da informação original *P*. De acordo com (KHAN, 1995), quanto maior for a complexidade da chave de criptografia, maior será o nível de segurança da informação.

Nesta dissertação, os termos "criptografar" e "codificar", bem como seus derivados, são tratados como sinônimos. Tratam da arte de tornar uma informação secreta. Logo, decriptografar ou decodificar e seus derivados são o antônimo disso.

Este trabalho está pautado na utilização da criptografia para a camada física do modelo de referência OSI. Na próxima seção, serão abordados os três principais tópicos relativos ao emprego da criptografia nesta camada.

2.2. Criptografia na Camada Óptica

Como mencionado no Capítulo 1, a literatura apresenta ao menos duas abordagens usuais a respeito de criptografia na camada óptica. São elas a criptografia quântica e a tecnologia OCDMA. Esta seção abordará os princípios de cada uma destas estratégias e, também, como uma variação de OCDMA pode ser utilizada para realizar a criptografia em TONs.

2.2.1. Criptografia Quântica

A criptografia quântica se baseia no fato de que a luz é constituída por pacotes chamados fótons. Esta técnica também permite que duas entidades que

queiram se comunicar, mesmo sem nunca terem trocado qualquer tipo de informação, possam estabelecer uma chave criptográfica única, utilizada para codificar e decodificar o sinal. A seguir, descreve-se um modelo para estabelecimento da chave criptográfica única entre as duas entidades, utilizado nesta técnica que é chamado BB84 (TANENBAUM, 2003). Este nome é uma referência às iniciais dos seus autores (Bennet e Brassard), seguido do ano da sua publicação (1984). A Fig. 2 apresenta um modelo teórico sobre essa técnica, para uma transmissão aleatória de 16 bits.

As duas entidades (o transmissor e o receptor) possuem cada uma dois conjuntos de filtros polarizadores. O primeiro destes conjuntos possui dois filtros perpendiculares, um horizontal e outro vertical, e define o que será chamado de base retilínea. O segundo destes conjuntos também é composto por dois filtros perpendiculares, mas está deslocado em 45º com relação ao primeiro conjunto e define o que será chamado de base diagonal.

Número do bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Informação Transmitida	0	0	1	1	1	0	1	0	1	1	0	0	0	1	0	1
Base Transmissor	⤢	↕	↘	↘	↔	↕	↔	↕	↘	↔	⤢	⤢	↕	↘	⤢	↘
Base Receptor	⤫	✢	✢	✢	✢	⤫	⤫	✢	✢	✢	⤫	⤫	⤫	✢	⤫	✢
Informação Recebida	⤢	↕	↕	↕	↔	↔	↔	↕	↘	↔	⤢	⤢	↕	↘	⤢	⤢
Base correta?	OK	OK	X	X	OK	X	X	OK	X	OK	OK	OK	X	X	OK	X
Chave Única	0	0			1			0		1	0	0			0	

Fig. 2 - Modelo teórico da atribuição de uma chave única na criptografia quântica.

Aleatoriamente, para cada uma dessas bases (a retilínea ou a diagonal) o transmissor atribui uma direção para o bit 0 e outra para o bit 1. Para efeitos ilustrativos, o transmissor escolhe para a base retilínea o filtro vertical para enviar o bit 0 e o filtro horizontal para enviar o bit 1. Da mesma forma, para a base diagonal, admite que o bit 0 será representado pelo filtro do canto inferior

esquerdo ao canto superior direito e o bit 1 o recíproco (TOWNSEND, 1998). Estas informações são enviadas ao receptor através de um texto simples.

O transmissor, a partir da sua pistola de fótons, gera uma onda contínua de luz (*Continuous Wave*, CW) e, para cada bit que ele deseja transmitir da sequencia aleatória inicial, atribui uma base de filtros. Após passar pelo filtro da base escolhida aleatoriamente, o fóton mantém a polarização determinada por aquele filtro. Ainda, vale destacar que o fóton não altera a sua polarização de transmissão inicial, após passar por um filtro polarizador. É importante notar que, se este mesmo fóton atravessar um segundo filtro polarizado a 45º em relação à sua própria polarização, seu novo estado de polarização se manterá ou será rotacionado em 90º com a mesma probabilidade.

O receptor possui um mesmo conjunto de filtros, conforme citado anteriomente (as bases retilínea ou diagonal). Da mesma forma, atribui aleatoriamente um desses conjuntos de filtros a cada bit recebido, que é representado por um fóton. Ou seja, o receptor terá uma sequência de bits recebidos que ele não sabe quais estão corretos ou não. A partir daí, o receptor informa ao transmissor em texto simples quais as bases que foram utilizadas para cada bit recebido. Analogamente, também em texto simples, o transmissor informa ao receptor se as bases utilizadas estão corretas ou não (TANEMBAUM, 2003). Desta forma, o receptor, a partir da informação das bases corretas utilizadas para identificar cada fóton recebido, consegue estabelecer uma chave que estatisticamente terá 50% do tamanho da sequência de bits inicial.

Um intruso, caso conseguisse furtar o sinal e receber essas informações, ainda assim erraria em 50% dos bits recebidos pelo receptor. Mesmo assim, é possível aumentar o grau de segurança desta chave criptográfica, aplicando a técnica de ampliação de privacidade, o que reduz ainda mais a chance do intruso reconhecer a chave estabelecida.

Muito embora a criptografia quântica seja considerada um método eficiente de codificar uma mensagem, ainda encontra-se em desenvolvimento e é de implementação complexa. Os custos de implantação da técnica são elevados, o que torna a sua utilização ainda muito restrita (KITAYAMA, 2011). Além disso, estudos indicam a efetividade da técnica para enlaces ópticos de até 97 km de extensão, o que pode ser um fator determinante para a sua aplicação. (TANAKA,2008; LADD, 2010).

2.2.2. Criptografia de Acesso Múltiplo por Divisão de Código Óptico (OCDMA)

O OCDMA é uma técnica de acesso múltiplo que permite que vários pares de usuários transmitam simultaneamente suas informações na mesma faixa de frequências (LOPES, 2005, HUISZOON, 2007). Em princípio, só é possível a recuperação do sinal transmitido caso o receptor conheça a chave de codificação utilizada pelo seu transmissor-par.

Uma das características desejáveis desta técnica é a maximização da ortogonalidade (incremento do grau de diferenciação entre os usuários) e da cardinalidade (quantidade de códigos disponíveis e utilizáveis). A técnica é considerada como de multiplexação estatística, pois sofre uma degradação maior à medida que aumenta a quantidade de usuários no sistema (SANTOS FILHO, 2006).

A Fig. 3 apresenta um esquemático de codificação no domínio do tempo (YIN, 2007). Numa transmissão convencional, (a) um bit é um pulso retangular

com duração T_b. Ao ser codificado, (b) este sinal é subdividido em N subintervalos T_c, denominados *chips*. Ou seja, cada *chip* T_c é composto de T_b/N subintervalos (REIS JR, 2009).

Cada bit, na transmissão *on-off keying* (OOK) convencional (a) é representado com apenas um pulso de sinal para o bit 1 e ausência de sinal para o bit 0. Após a codificação (b), o bit 1 é representado pelo número de *chips* iluminados w, modulados na freqüência λ_0 que é uma freqüência mais alta do que a do sinal original. Os *chips* iluminados w aparecem destacados na figura. Por outro lado, o bit 0 não sofre alterações – ou seja, continua sendo representado pela ausência de sinal (REIS JR, 2009).

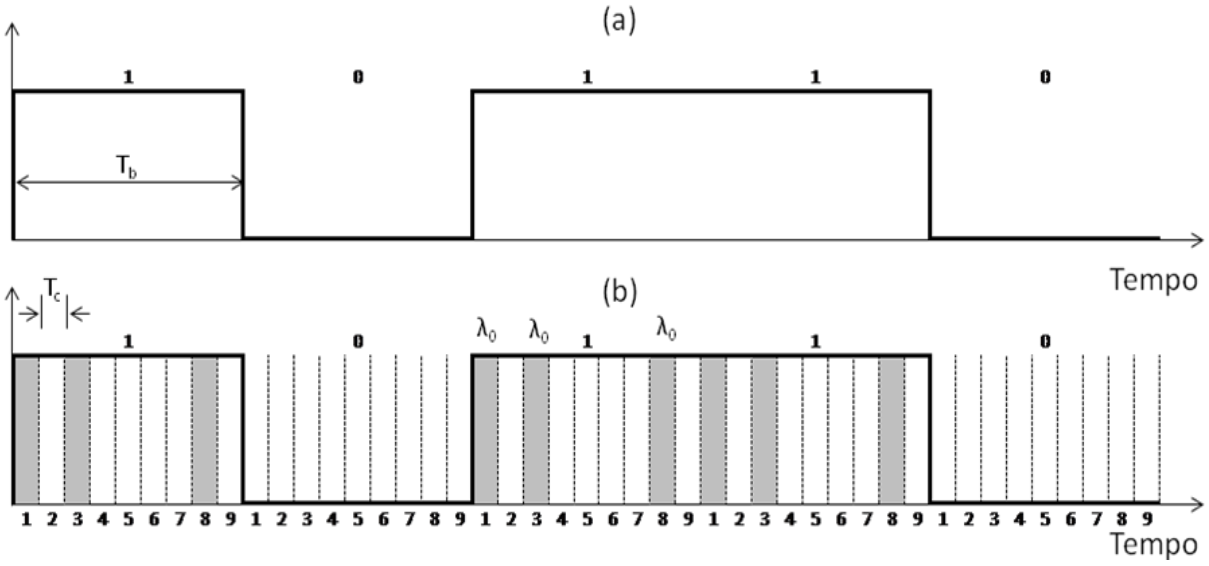


Fig. 3 - Modelo de codificação OCDMA no domínio do tempo, para N= 9 e w= 3.

Na Fig. 4 mostra-se o diagrama de blocos da codificação do sinal no domínio do tempo, utilizando-se linhas de atraso óptico (*Optical Delay Line*, ODL). O sinal na entrada do codificador é dividido em três partes (três é um número ilustrativo apenas). Cada uma dessas três partes é submetida a um atraso próprio, τ_i. Na saída do codificador estas fatias são multiplexadas e o sinal

resultante é transmitido para uma rede óptica que, na maioria das vezes, é considerada uma rede de acesso (ABDALLAH, 2011).

No lado do receptor, a decodificação do sinal utiliza os mesmos equipamentos que a codificação, sendo que os atrasos são ajustados para recompor o sinal original. Os parâmetros λ_0, w e N são combinados, gerando a máscara do sinal. O receptor correlaciona a máscara do sinal, com o seu código, analisando o grau de similaridade entre os dois. Se o sinal transmitido e a máscara do receptor forem idênticos, a autocorrelação é elevada e o sinal é devidamente recuperado. (SANTOS FILHO, 2006).

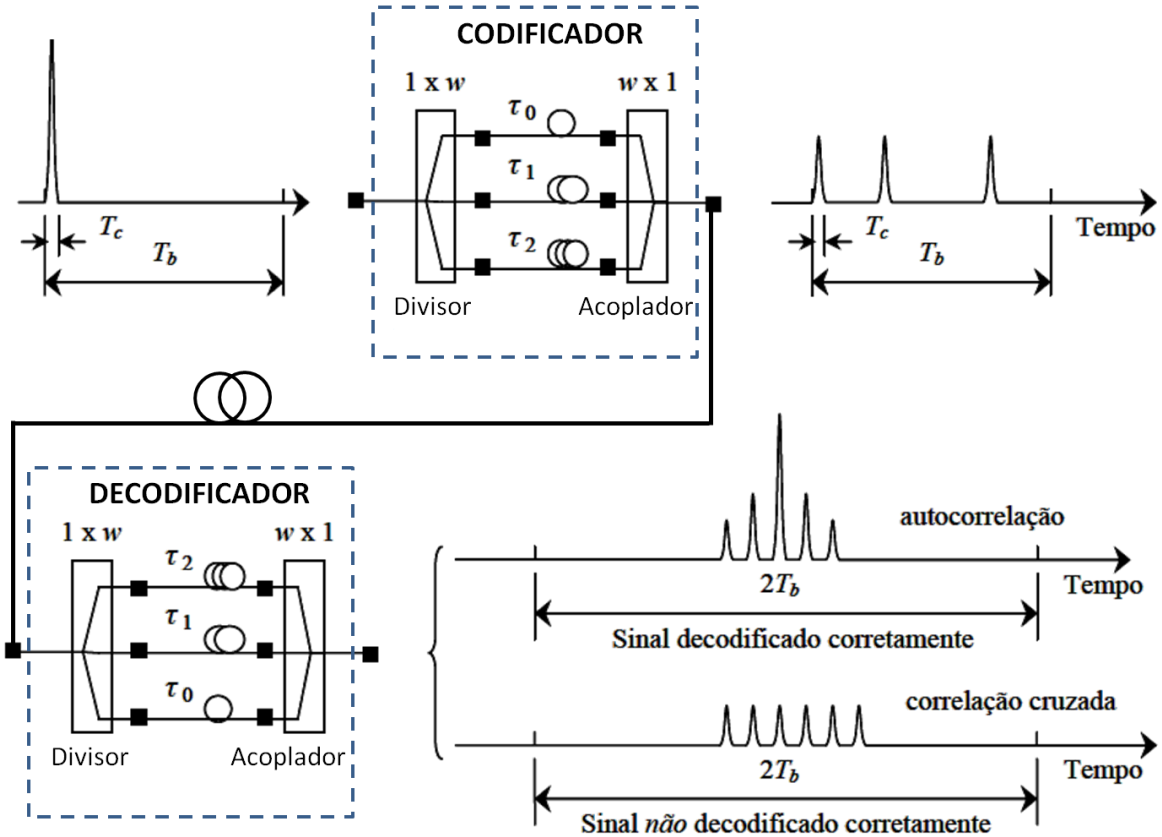


Fig. 4 - Diagrama de blocos do Codificador e Decodificador OCDMA

Na literatura são apresentadas outras técnicas de OCDMA, tais como as codificações coerentes e 2D. No entanto, uma abordagem detalhada destas outras técnicas está além do escopo deste trabalho e pode ser encontrada em (YIN, 2007).

As implementações do OCDMA mencionadas nesta seção provocam o alargamento espectral do sinal codificado, que é aceitável para permitir a transmissão simultânea de dados em redes de múltiplo acesso. Em contrapartida, tal alargamento não seria aconselhável para criptografar sinais em redes *core*. Isto se deve ao fato de que estas redes empregam a tecnologia WDM, utilizando equipamentos que limitam a banda dos canais à uma largura fixa e que, como no caso de filtros, multiplexadores e demultiplexadores, não aceitariam sinais com o espectro alargado.

2.2.3. Criptografia OCDMA no domínio da freqüência

A técnica da codificação espectral OCDMA por diferenciação de fase, resultante da aplicação de uma máscara de difração dispersiva de Bragg *M* (CORNEJO, 2007) é ilustrada na Fig. 5. O sinal óptico que incide sobre uma grade de difração GD_1 é separado espacialmente em diferentes componentes espectrais. Este sinal é refletido pela grade e transmitido a uma lente convergente. A partir daí, este sinal é submetido a uma máscara de difração dispersiva de Bragg *M*, composta de vários *pixels* que filtram parte das componentes do sinal. A fase de cada componente é então variada através de uma tensão aplicada a cada *pixel*. Nota-se que a variação da fase é proporcional da uma fração do período da portadora. A variação de fase a que cada componente espectral é submetida induz um alargamento temporal que distorce o

sinal, dificultando que possíveis espiões tenham acesso à informação. O sinal é, então, transmitido para outra lente convergente e multiplexado na grade de difração GD_2, resultando num sinal codificado (SANTOS FILHO, 2006).

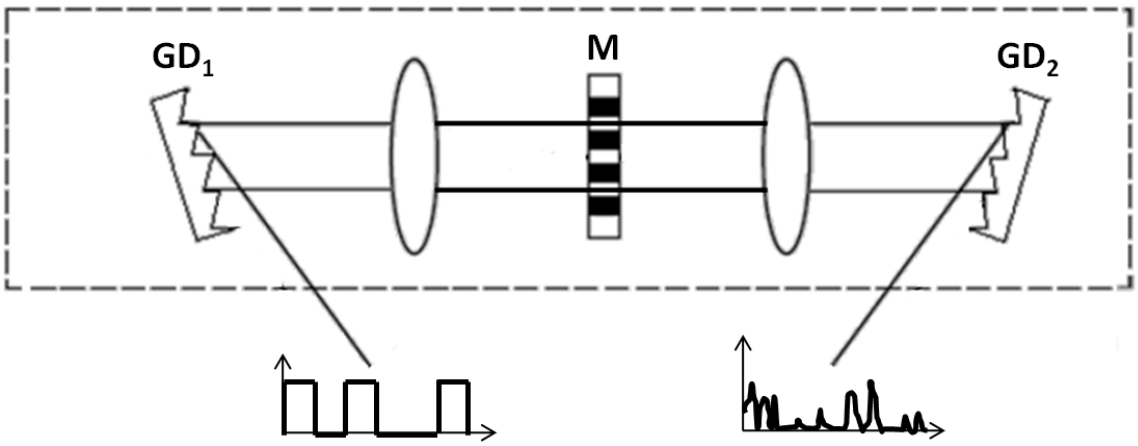


Fig. 5 - Codificação OCDMA por diferenciação de fase.

O tamanho e o número de *pixels*, combinados com o nível de tensão a que cada um destes dispositivos é submetido, constituem a chave de codificação do sinal (CORNEJO, 2007). A decodificação do sinal é obtida pelo mesmo conjunto de equipamentos, com aplicação de tensões nos pixels que conduzam a uma fase complementar àquela utilizada no codificador.

Esta técnica, assim como a considerada nesta dissertação (ver próximo capítulo) não gera alargamento espectral do sinal e é utilizada para criptografar canais individuais de sistemas WDM. As principais diferenças entre ambas as técnicas serão abordadas no próximo capítulo.

3. CRIPTOGRAFIA ÓPTICA POR FATIAMENTO ESPECTRAL

No capítulo anterior, apresentou-se o conceito de criptografia óptica e a aplicação dessa técnica às TONs. Foram descritos os conceitos básicos das criptografias quântica e óptica em redes com acesso múltiplo por divisão de código. Neste capítulo, apresentaremos na Seção 3.1 a descrição da técnica de criptografia do sinal óptico por fatiamento espectral utilizada nessas simulações. Já na Seção 3.2, encerraremos o capítulo descrevendo o arranjo das simulações que nortearam este trabalho.

3.1. Descrição da Técnica de Criptografia Óptica por Fatiamento Espectral

Os sistemas de codificação e decodificação do sinal têm o seu diagrama de blocos ilustrados na Fig. 6.

O sinal óptico na entrada do codificador é dividido em *n* fatias espectrais, através da aplicação de um demultiplexador óptico ou de uma combinação de um *splitter* e filtros ópticos, com uma largura de banda estreita o suficiente para atingirmos a dimensão da fatia espectral desejada. À *i*-ésima destas fatias espectrais, que podem possuir larguras de banda distintas, é atribuída uma

atenuação α_i e um atraso τ_i. Considera-se que a atenuação e o atraso máximos aplicados a cada fatia espectral são, respectivamente, α_{max} e τ_{max}.

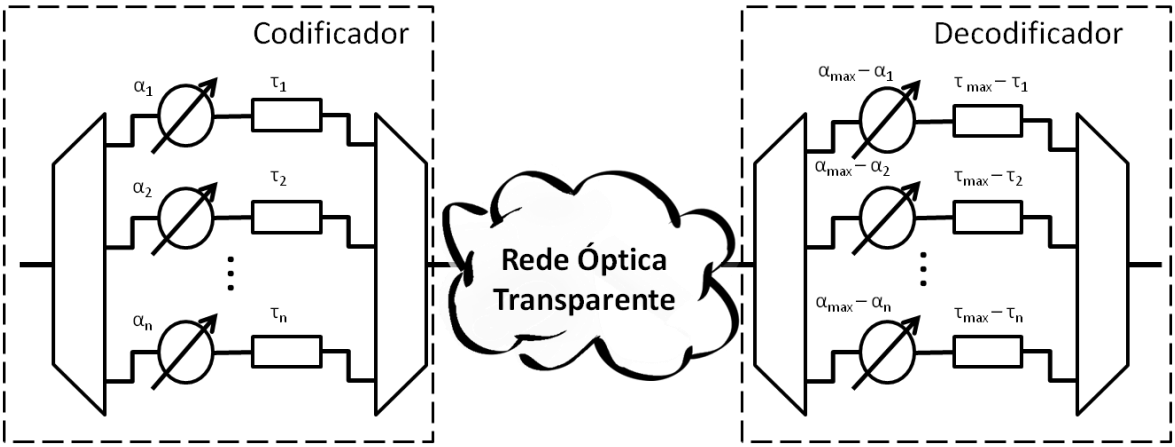


Fig. 6 - Diagrama de Blocos do Codificador e do Decodificador.

A Fig. 7 apresenta um diagrama conceitual do fatiamento espectral e como a aplicação dos atributos de atenuação α e atraso τ modificam o espectro do sinal óptico (ABBADE, 2012). A robustez do sistema de criptografia considerada neste trabalho está ligada à combinação da quantidade e da largura dessas fatias espectrais e dos valores de atenuação e atraso que são aplicados a cada uma delas. De fato, quanto maior o número de variáveis espera-se que maior seja a complexidade da chave criptográfica e, consequentemente, a confidencialidade da informação.

Todas estas fatias espectrais são recombinadas através do uso de um multiplexador óptico ou de um acoplador óptico, cuja função é compor o sinal que será transmitido para a TON. Cabe salientar que neste ponto, o sinal óptico estará idealmente ininteligível. Uma maneira de avaliar a qualidade da criptografia utilizada é medir a BER do sinal criptografado, BER_C. Cabe destacar que a maior BER possível em um sinal binário é 50%. Se, por exemplo, esta taxa de erro fosse de 60%, bastaria conectar um inversor de bits na saída do sinal para reduzí-la a 40% (ABBADE, 2012).

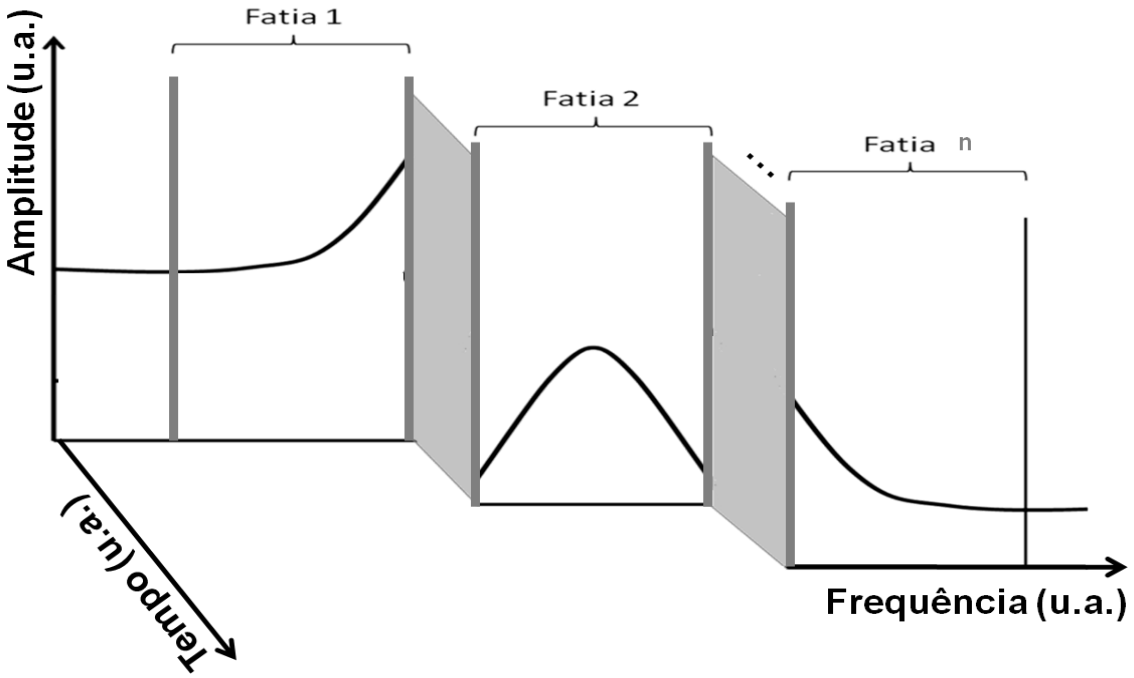


Fig. 7 – Modelo teórico de distorção do espectro óptico por fatiamento espectral.

Na saída do codificador, as fatias espectrais são multiplexadas e transmitidas pela TON. A partir daí, o sinal é recebido no circuito decodificador, que possui a mesma estrutura física do circuito que codificou o sinal original. A aplicação dos fatores de atenuação e atraso neste sinal distorcido é ajustada para a reconstrução do sinal óptico gerado pelo transmissor. Tal recurso deve ser aplicado à *i*-ésima fatia espectral, que será submetida a uma atenuação $\alpha_{max} - \alpha_i$ e a um atraso $\tau_{max} - \tau_i$, recompondo-se o sinal óptico original. Neste ponto, o sinal óptico estará idealmente recuperado e uma maneira de avaliar a eficiência da técnica utilizada é medir a BER do sinal nesse ponto, BER_D. Considerou-se, que a BER_D na saída do decodificador deveria ser menor ou igual a 10^{-9}, requisito comum em sistemas de comunicações ópticas sem correção antecipada de erros (*Foward Error Correction*, FEC) (YONENAGA, 1997).

Os circuitos do codificador e decodificador apresentados na Fig. 6 são constituídos de elementos disponíveis comercialmente e podem ser implementados com diversas tecnologias. Para a fabricação destes circuitos,

poderiam ser empregados componentes discretos: atenuadores variáveis e linhas ópticas de retardo (*Optical Delay Line*, ODL), que implementam com simplicidade atrasos superiores a um período de bit. Também, seria possível a utilização da fotônica de silício para a construção integrada destes dispositivos (HORST, 2011).

Outro ponto importante para se atingir a segurança da chave criptográfica é a quantidade requerida de fatias espectrais para distorção do sinal. Quanto maior a quantidade de fatias espectrais, mais complexa será a chave criptográfica e mais robusto se torna o sistema. De acordo com (GERSTEL, 2012), há tecnologia disponível para a construção de filtros ópticos sintonizáveis com largura de banda tão estreitos quanto 6.25 GHz. Ou seja, considerando-se sinais que ocupem uma banda próxima de 50 GHz (em consonância com o espaçamento típico entre canais colocados na grade do ITU-T (ITU-T G.692)) teremos a possibilidade de aplicar até 8 fatias espectrais com atenuações e atrasos próprios para cada canal transmitido. A combinação em série de um conjunto de filtros sintonizados com certo desvio em relação às suas freqüências centrais, em teoria, permitiria que esta largura espectral fosse ainda reduzida.

Não obstante, cabe destaque que a empresa Finisar, renomada fabricante de equipamentos e dispositivos ópticos, produz um equipamento chamado *Wave Shaper*®, WS (Em: <http://www.finisar.com/WaveShaper>. Acesso em: 30 julho 2012). O equipamento, que trabalha com a técnica de comutação seletiva de comprimento de ondas (*wavelength selective switches*, WSS) é construído com tecnologia de cristal líquido sobre silício (*liquid crystal on silicon*, LCoS), e é capaz de fatiar o espectro óptico em sub-bandas de 10 GHz, permitindo o ajuste destas larguras de banda e das atenuações aplicadas a cada segmento (FALTA, 2012).

Ainda, observa-se que apesar deste trabalho apresentar nos capítulos posteriores os resultados das simulações para sinais ópticos com modulações de não retorno ao zero com chaveamento *on-off* (*Non Return to Zero, On-Off*

Keying, NRZ-OOK) e chaveamento por deslocamento de quadratura de fase diferencial (*Differential Quadrature Phase Shift Keying,* DQPSK) à taxa de 40 Gbps, em princípio, a técnica proposta é transparente ao formato de modulação utilizado e à taxa de transmissão de dados.

É importante destacar as diferenças entre esta técnica e aquela considerada em (CORNEJO, 2007). Primeiramente, observa-se que esta técnica apresenta a modificação dos parâmetros de amplitude e atraso das fatias espectrais, que pode variar entre um ou mais períodos de bit, para codificação do sinal. Já a outra técnica, utiliza o atraso de fase das componentes de dada fatia espectral com esta mesma finalidade.

Outra diferença observada entre as técnicas é que em (CORNEJO, 2007) não utiliza métricas para avaliar o nível de criptografia atingida na saída do codificador. Na técnica proposta, a avaliação é feita medindo-se a BER do sinal codificado, BER_C. Também verifica-se que a técnica de (CORNEJO, 2007) analisa sinais NRZ-OOK a uma taxa de 10 Gbps, enquanto esta técnica já inclui a avaliação da modulação DQPSK, à taxa de 40 Gbps.

Por fim, a técnica proposta considera o emprego de filtros com bandas próximas às dos filtros que estão comercialmente disponíveis, enquanto em (CORNEJO, 2007), é considerada a utilização de filtros com banda muito inferiores a estas. Na próxima seção, efetua-se a descrição do arranjo de simulação considerado para a obtenção dos resultados deste trabalho.

3.2. Arranjos das Simulações

A Fig. 8 ilustra o diagrama de blocos do arranjo utilizado nas simulações, que foram executadas com a versão 8.7 do software VPITransmissionMaker, da empresa VPIPhotonics Inc. Para tanto, um sinal com modulação NRZ-OOK ou DQPSK é gerado numa sequência aleatória de 2048 bits, com uma potência de pico de 0 dBm. A este sinal é aplicado um ganho G_1, com o objetivo de manter este mesmo nível de potência de pico na saída do codificador. O sinal é transmitido pelo codificador, quando então recebe a chave criptográfica, conforme explanação anterior. Após codificado e multiplexado, o sinal resultante então é propagado através da TON por um enlace de comprimento *L*.

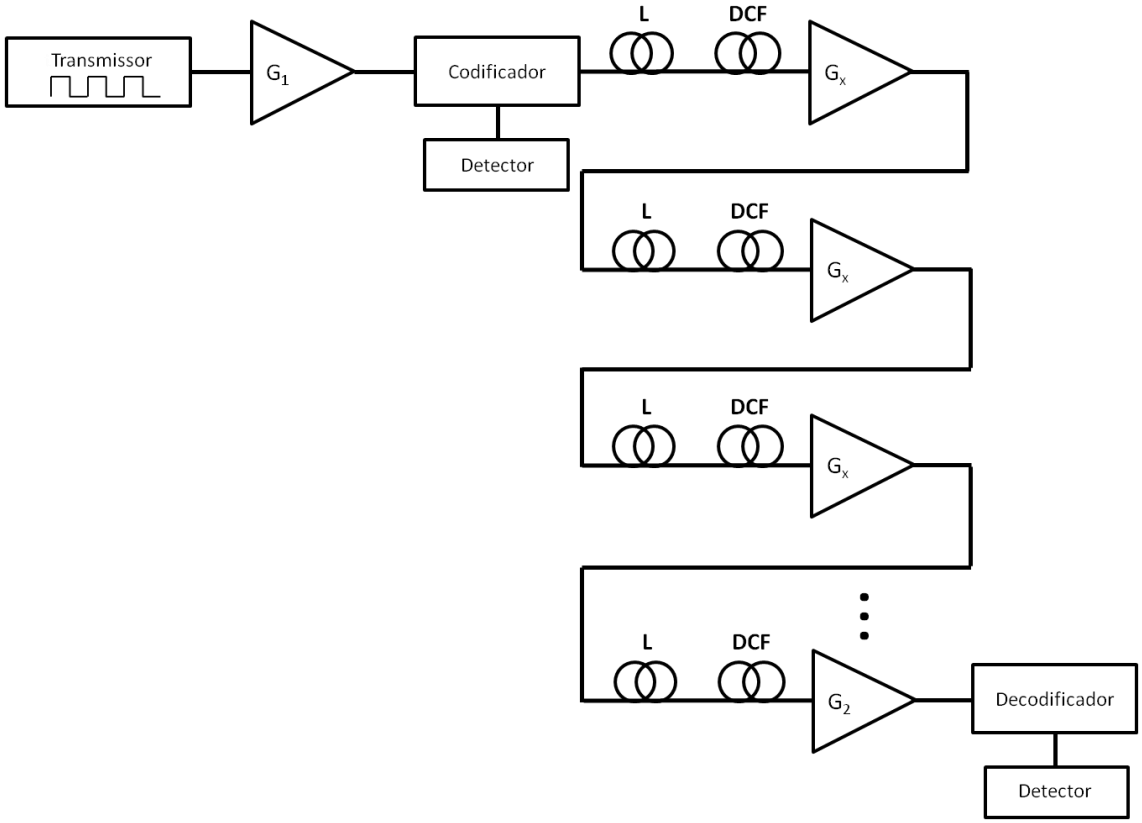


Figura 8 - Diagrama de Blocos do Arranjo Experimental.

Na propagação do sinal, foram utilizados enlaces ópticos compostos de fibra padrão monomodo com *L*= 40 km, e coeficiente de dispersão D_{SMF}= 16 ps/(km.nm) e também uma fibra para compensação da dispersão (*dispersion compensating fiber*, DCF), com o objetivo de se efetuar a compensação dos

efeitos do alargamento de pulso no enlace. Esta fibra, por sua vez, têm o coeficiente de dispersão negativo D_{DCF}= -90 ps/(km.nm) e possui um comprimento, L_{DCF}, calculado para compensar exatamente a dispersão introduzida pela fibra de propagação, mostrado a seguir:

$$L_{DFC} = \left| L\left(\frac{D_{SMF}}{D_{DCF}}\right)\right| \qquad (1)$$

Além disso, a cada enlace, é aplicado um ganho G_x, com o objetivo de compensar a atenuação sofrida pelo sinal em cada enlace de propagação. Para tanto, foi utilizado um modelo que simula um amplificador de fibra dopada a Érbio (*Erbium Doped Fiber Amplifier*, EDFA) com figura de ruído de 4 dB.

O circuito decodificador ou de criptoanálise amplifica o sinal recebido por um fator G_2, que têm como objetivo a compensação da atenuação no último enlace de propagação e a manutenção do nível de 0 dBm na saída do decodificador. Desta forma, dada a equalização das potências nas saídas do codificador e do decodificador, as BERs nestes dois dispositivos podem ser comparadas adequadamente após a fotodetecção do sinal óptico.

Para simplificar a avaliação da influência das variações de α e τ no sinal óptico, foram inicialmente consideradas apenas três fatias espectrais. Para a modulação NRZ-OOK, a largura de banda utilizada para cada fatia foi de 40 GHz, totalizando 120 GHz. Para a modulação DQPSK, foi utilizada uma banda total de 60 GHz, composta de três fatias de largura simétrica de 20 GHz. Posteriormente, outras simulações foram executadas considerando os fatiamentos do espectro óptico dentro do limite de banda de 50 GHz da grade de recomendação do ITU-T para sinais com taxa de 40 Gbps.

Por se tratar de um primeiro estudo sobre a BER da técnica, todos os filtros considerados neste trabalho têm um perfil ideal (retangular). A influência de filtros com perfil similar ao dos comercialmente utilizados atualmente será investigada em (SILVA, 2012).

No próximo capítulo, são apresentados os resultados obtidos durante as simulações. Em especial, são mostrados os espectros ópticos do sinal na entrada do codificador, do sinal codificado e, posteriormente, decodificado. Também efetua-se uma análise da ação da técnica no domínio do tempo, sendo apresentados os resultados obtidos para uma sequência pré-definida de bits. Por fim, faz-se a avaliação da influência da propagação e da redução da largura das fatias espectrais na qualidade do sinal recuperado na saída do decodificador, comparando os resultados obtidos para as modulações NRZ-OOK e DQPSK.

4. RESULTADOS

A técnica de criptografia óptica analisada neste trabalho foi descrita no Capítulo 3. Neste capítulo, serão apresentados os resultados obtidos durante as simulações para sinais NRZ-OOK e DQPSK à 40 Gbps, respectivamente, nas Seções 4.1 e 4.2. Em particular, serão consideradas em cada uma destas seções as análises espectral e temporal do sinal óptico, incluindo a influência da atenuação e do atraso das fatias espectrais na BER. Todas as análises, a não ser em casos explicitamente indicados ao longo do texto, basearam-se em simulações de 2048 bits. Além disso, também será avaliada a propagação destes sinais por enlaces de 40 km, até uma distância total de propagação de 400 km, relativa a 10 enlaces. Por fim, na Seção 4.3 será avaliado o impacto da redução da largura de banda das fatias espectrais no desempenho dos sinais codificados e decodificados e na Seção 4.4 serão comparados os resultados obtidos para as modulações NRZ-OOK e DQPSK.

4.1. Sinais NRZ-OOK

4.1.1. Análises Espectral e Temporal

A Fig. 9 ilustra o espectro óptico do sinal NRZ-OOK na entrada do codificador (a), conforme apresentado no diagrama de blocos da Fig. 6. A resolução espectral utilizada na simulação foi de 5 MHz. Nela observa-se a

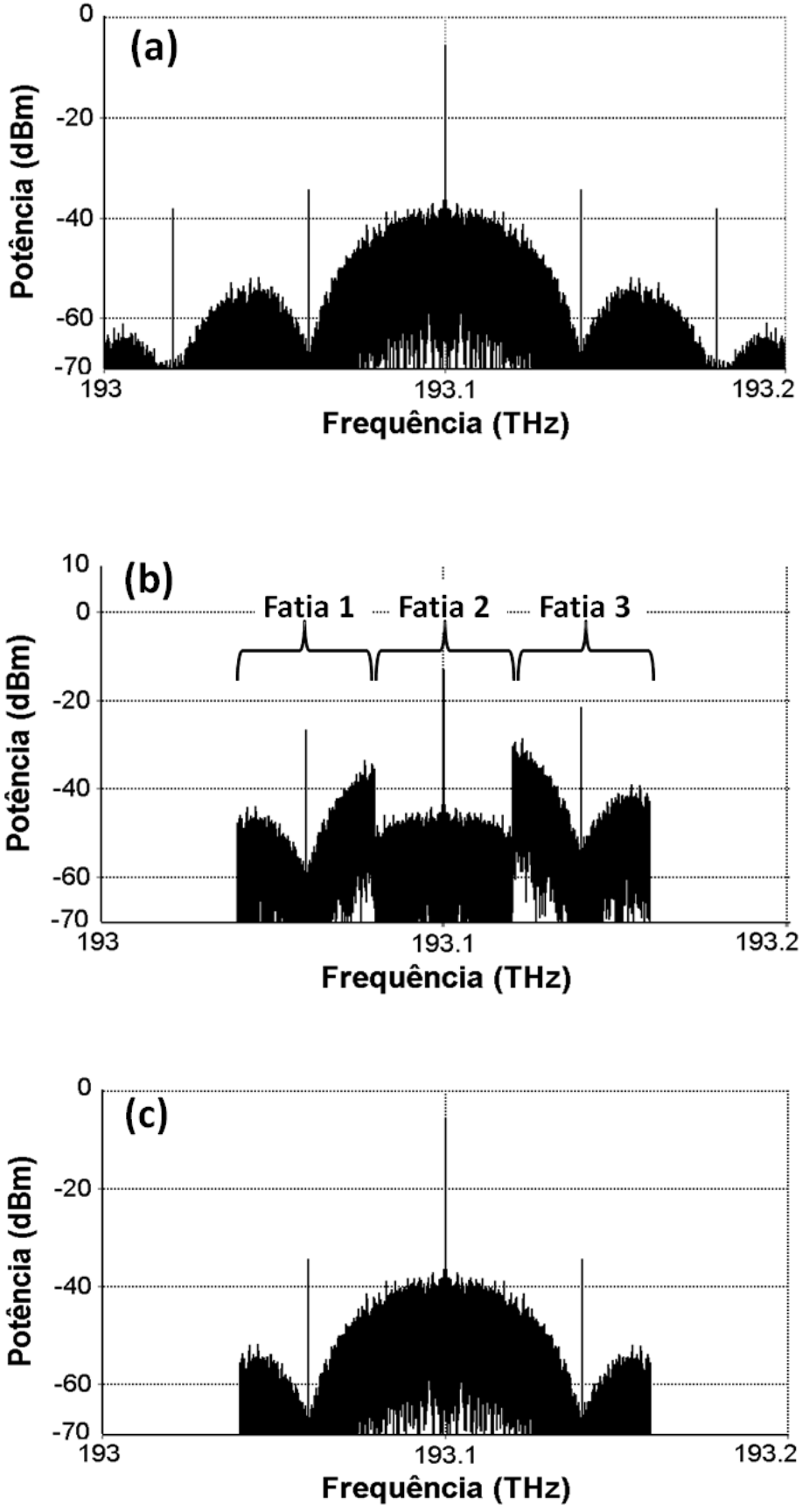


Fig. 9 – Sinal NRZ-OOK. Espectro Óptico (a) na entrada do codificador; (b) na saída do codificador, para $\alpha_1 = 5$, $\alpha_2 = 20$ e $\alpha_3 = 0$ dB; $\tau_1 = \tau_2 = \tau_3 = 0$ ps.; e (c) na saída do codificador.

portadora centrada em 193.1 THz e componentes espectrais mais significativas espaçadas da portadora por múltiplos de 40 GHz.

Nessa mesma figura (Fig. 9), ilustra-se o espectro óptico do sinal na saída do codificador (b). Nota-se o sinal óptico já fatiado, neste caso com atenuações de $\alpha_1 = 5$ dB, $\alpha_2 = 20$ dB e $\alpha_3 = 0$ dB. Nesta situação, não foram aplicados atrasos às fatias espectrais ($\tau_1 = \tau_2 = \tau_3 = 0$ ps). Cada fatia espectral possui largura de banda de 40 GHz e todo o sinal óptico que está fora da faixa de 193.04 e 193.16 THz foi eliminado devido a aplicação dos filtros de perfil retangular, responsáveis também pelas variações abruptas na amplitude do sinal durante as transições entre estas fatias. Por fim, apresenta-se o espectro óptico do sinal recuperado na saída do decodificador (c) do mesmo diagrama de blocos da Fig. 6. Da mesma forma que a figura anterior (b), o sinal óptico que se encontra fora da faixa de 193.04 e 194.16 THz foi suprimido dada a aplicação dos filtros nos blocos de codificação e decodificação. Entretanto, observa-se que dentro desta faixa de frequências, o sinal é muito próximo àquele apresentado no espectro do sinal original (a). As supressões das componentes laterais do espectro não influenciam na qualidade do sinal verificado na saída do decodificador, uma vez que suas amplitudes não possuem valores expressivos. De fato, as simulações indicam que este sinal possui BER_D inferior a 10^{-15} e pode, portanto, ser considerado livre de erros.

Os diagramas de olho relativos ao sinal óptico gerado para os sinais (a) na entrada do codificador, (b) codificado e (c) decodificado, para uma sequência pseudoaleatória de 2048 bits, são ilustrados na Fig. 10. Neste caso, foram aplicadas atenuações de $\alpha_1 = 5$ dB, $\alpha_2 = 20$ dB e $\alpha_3 = 0$ dB e atrasos $\tau_1 = \tau_2 = \tau_3 = 0$ ps. Conforme esperado, o diagrama de olho do sinal codificado (b) apresenta-se fechado e ininteligível, enquanto o diagrama de olho do sinal decodificado (c) apresenta-se aberto e bem definido. Conforme mencionado anteriormente, este sinal pode ser considerado livre de erros, pois sua BER_D é inferior a 10^{-15}.

A seguir, analisa-se a ação da técnica proposta no domínio do tempo. Para tanto, foi gerada uma seqüência aleatória de 28 bits pré-definidos, relativa aos sinais de entrada, codificado e decodificado. As condições de codificação do sinal são idênticas às apresentadas nos estudos anteriores.

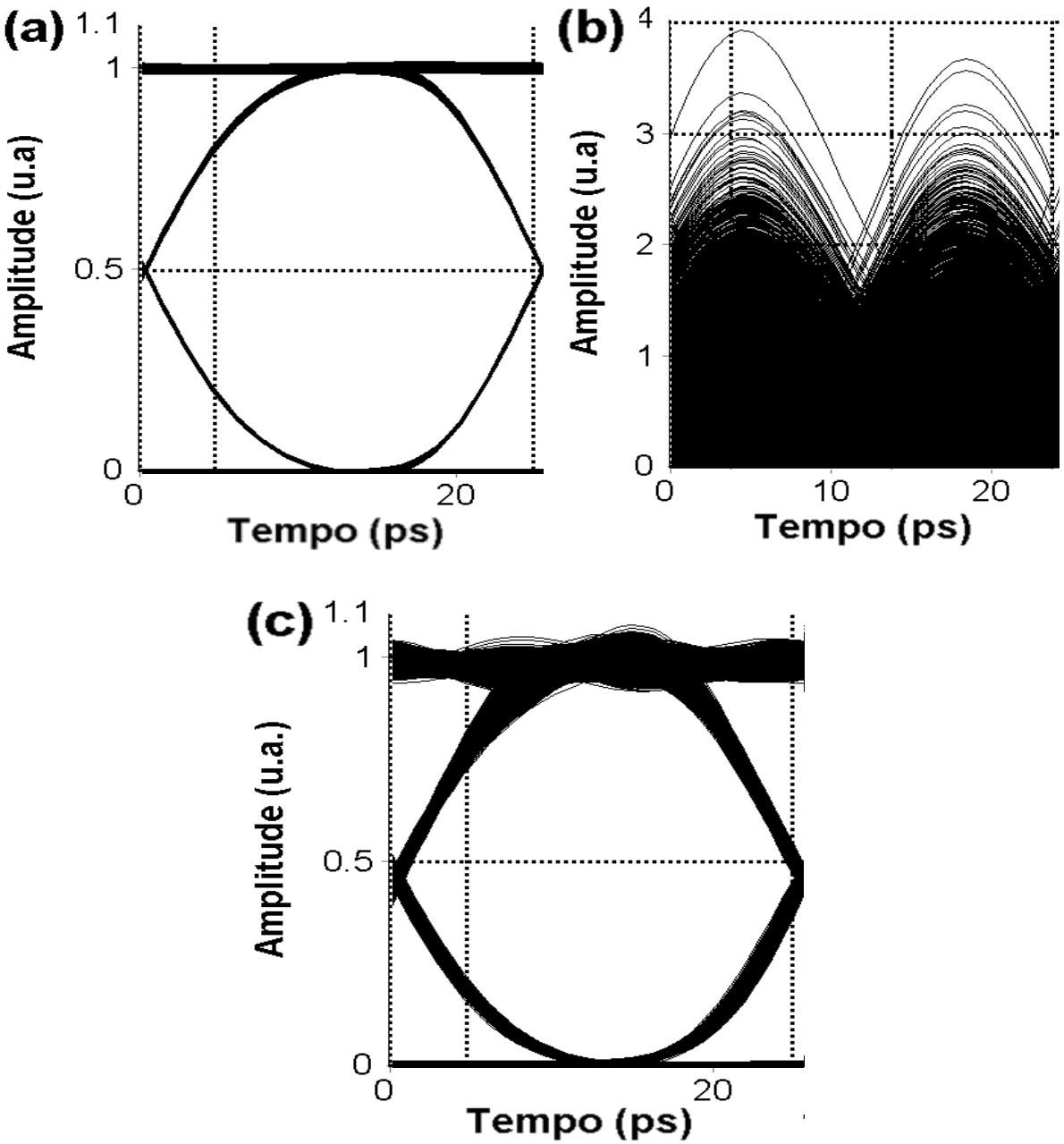


Fig. 10 – Sinal NRZ-OOK. Diagramas de Olho do sinal (a) na entrada do codificador; (b) na saída do codificador; e (c) na saída do decodificador, para $\alpha_1 = 5$, $\alpha_2 = 20$ e $\alpha_3 = 0$ dB; $\tau_1 = \tau_2 = \tau_3 = 0$ ps.

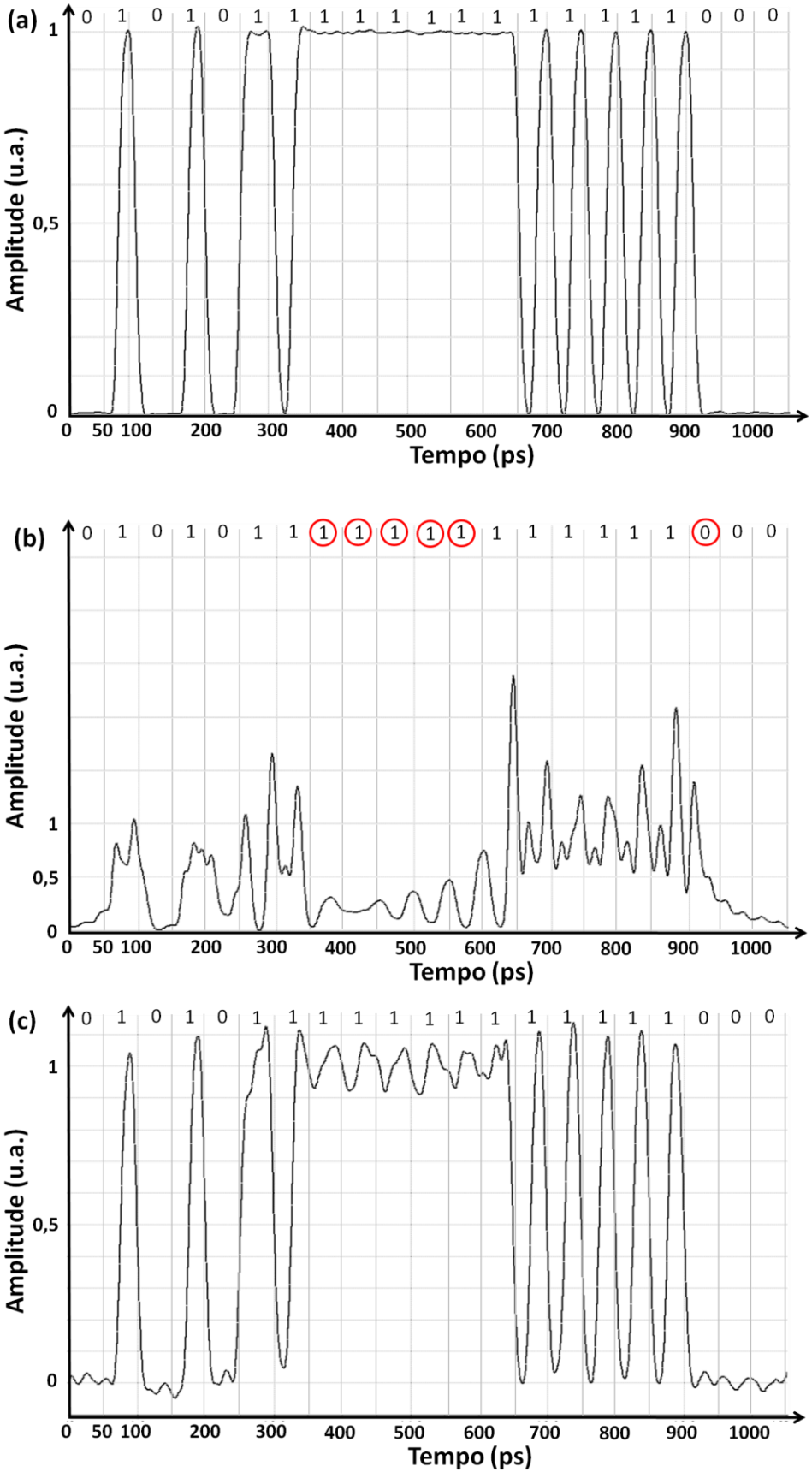


Fig. 11 – Sinal NRZ-OOK. Sequência de Bits do sinal (a) na entrada do codificador, (b) codificado e (c) decodificado, para $\alpha_1 = 5$, $\alpha_2 = 20$ e $\alpha_3 = 0$ dB; $\tau_1 = \tau_2 = \tau_3 = 0$ ps.

A Fig. 11 ilustra a sequência temporal dos 28 bits (a) na entrada do codificador, (b) na saída do codificador e (c) na saída do decodificador. Cada bit possui a duração de 25 ps. Os níveis alto e baixo do sinal na entrada do codificador (a) são muito bem definidos. Após a codificação (b) observa-se uma versão bem distorcida do sinal de entrada do codificador, assemelhando-se a um sinal analógico. É possível a verificação de alguns bits errados (destacados com um círculo na figura) com relação ao sinal de entrada. Neste caso, constatou-se 6 bits errados de um total de 21 bits gerados, o que significa uma BER_C estimada de 29%. A BER estimada quando se expande esta simulação para uma sequência aleatória de 2048 bits é de 33%.

Já o sinal decodificado (c), apresenta a mesma forma do sinal de entrada, com pequenas oscilações do nível alto que estão associadas à eliminação das fatias espectrais que estão fora da banda compreendida entre 193.04 e 193.16 THz. Tais distorções não são significativas e, da mesma forma que no caso anteriormente citado, pode ser considerado um sinal idealmente livre de erros ($BER_D < 10^{-15}$).

4.1.2. Influência da Atenuação das Fatias Espectrais na BER

Na Fig. 12, temos a variação da BER_C em função da aplicação da atenuação na fatia espectral central, combinada com atenuações nas fatias espectrais laterais, para as seguintes situações:

a) $\alpha_1 = 0$ dB; $\alpha_3 = 5$ dB
b) $\alpha_1 = \alpha_3 = 0$ dB e
c) $\alpha_1 = 5$ dB; $\alpha_3 = 0$ dB.

Observa-se um incremento da BER_C em função do aumento da atenuação na fatia central α_2. A BER_C tem um aumento expressivo à medida que há um crescimento de α_2, e assume um comportamento assintótico para α_2 > 15 dB. Nota-se também uma sobreposição entre as situações (a) e (c), relativas às atenuações nas fatias laterais α_1 e α_3, devido a simetria entre estas fatias espectrais.

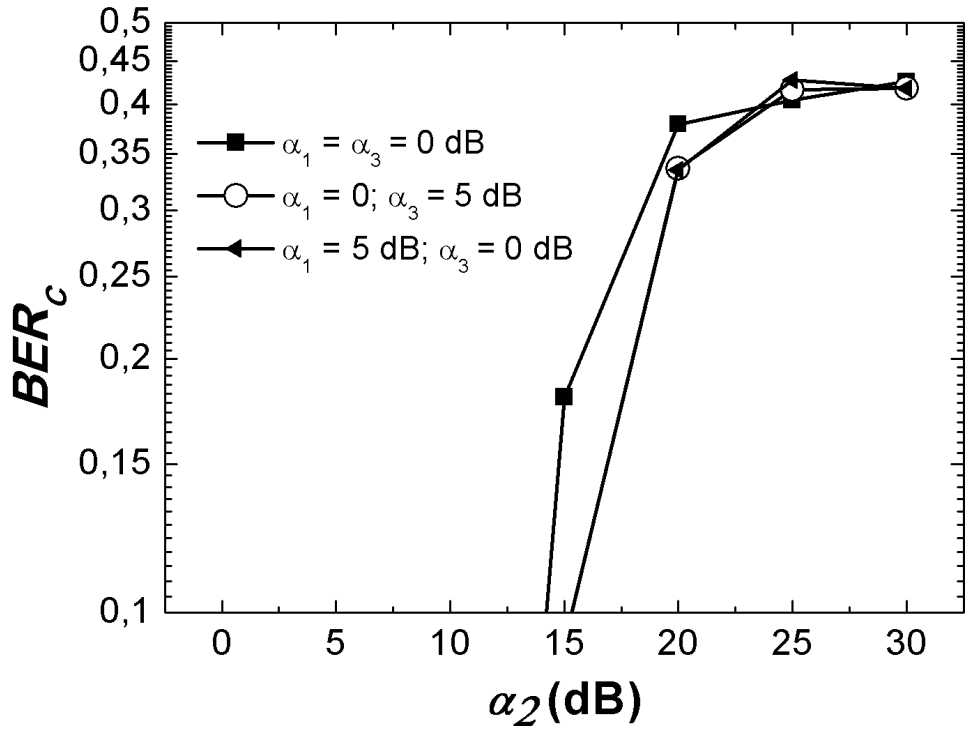


Fig. 12 – Dependência entre a BER_C do sinal codificado e α_2 para diferentes atenuações das fatias α_1 e α_3.

Também se destaca que a atenuação nas fatias laterais, combinadas com a atenuação α_2, causam uma BER_C inferior àquela das atenuações aplicadas apenas à fatia central α_2, até α_2 = 20 dB. Isto se deve ao fato de que, nesta situação, há uma redução na diferença de potências entre as fatias espectrais central e lateral, implicando, portanto, numa menor degradação do espectro óptico do sinal. Quando α_2 > 20 dB, observa-se uma alternância nestes resultados.

4.1.3. Influência do Atraso das Fatias Espectrais na BER

A Fig. 13 mostra a variação da BER_C em função da aplicação do atraso nas fatias espectrais central e laterais, para $\alpha_1 = \alpha_2 = \alpha_3 = 0$ dB, para os seguintes casos:

a) $\tau_1 = \tau_3 = 0$ ps, τ_2 variando
b) $\tau_2 = \tau_3 = 0$ ps, τ_1 variando
c) $\tau_1 = \tau_2 = 0$ ps, τ_3 variando

Na situação (a), observa-se um incremento de BER_C em função do aumento do atraso na fatia central τ_2, até dois períodos de bits, ou seja, 50 ps. A partir daí, o incremento do atraso é assintótico e não causa variações expressivas na BER_C. Como era de se esperar, dada a simetria das fatias espectrais 1 e 3, as curvas referentes às situações (b) e (c) relativas aos respectivos atrasos de τ_1 e τ_3, são praticamente sobrepostas, devido à semelhança dos seus resultados quantitativos. Também, o incremento de BER_C em função da aplicação dos atrasos nas fatias espectrais laterais (situações (b) e (c)) são menos significantes quando comparados aos resultados obtidos na aplicação dos mesmos atrasos na fatia central (curva (a)). Isso ocorre porque na fatia espectral central há uma maior concentração da energia do sinal. Quando é utilizado atraso simultaneamente a uma fatia espectral já atenuada, não se verifica um incremento significativo na grandeza da BER_C. Os resultados destas simulações são mostrados na próxima Seção.

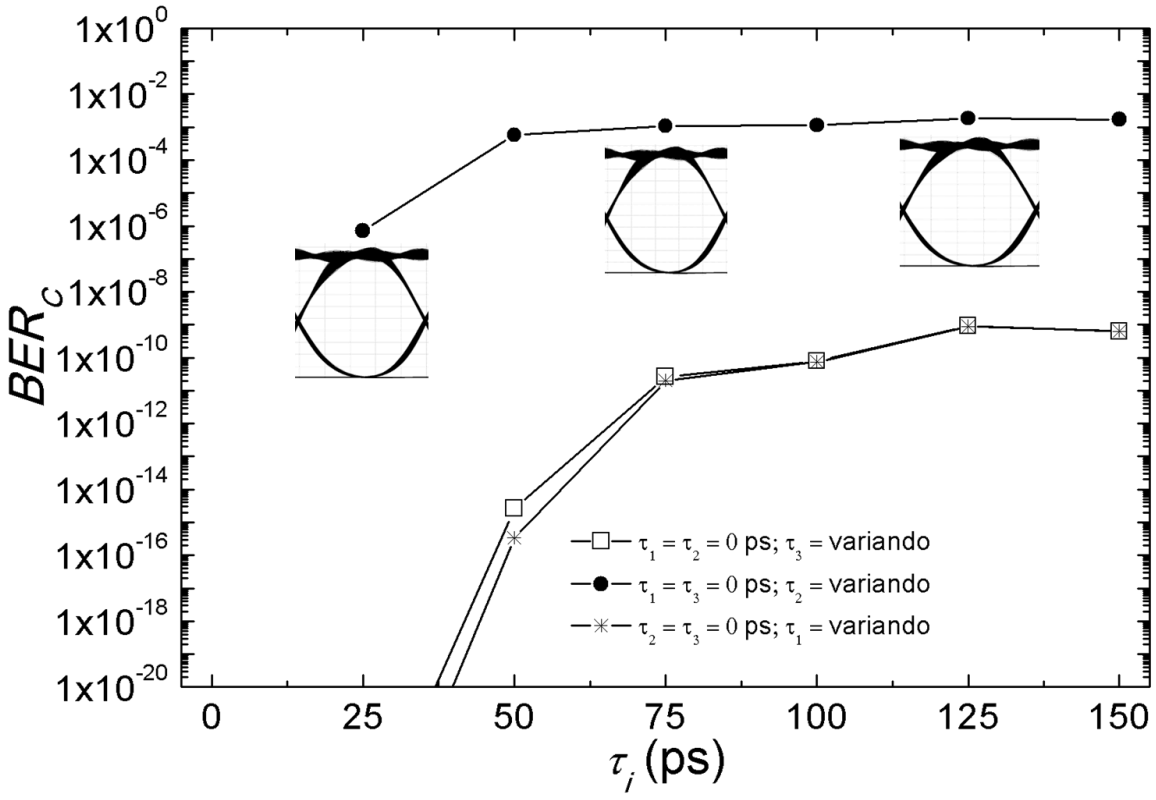


Fig. 13 – BER_C em função do incremento de τ_1, τ_2 e τ_3.

4.1.4. Avaliação da BER em Função da Propagação do Sinal Óptico

Os testes foram realizados conforme o diagrama de blocos apresentado na Fig. 6, com até 10 enlaces de 40 km cada. Em todos os casos, é possível obter no decodificador o sinal recuperado e praticamente livre de erros, pois $BER_D < 10^{-15}$, que, em princípio, seria muito difícil de ser medida. No entanto, para fins ilustrativos, a Fig. 14 apresenta os resultados obtidos BER_D, para possibilitar uma comparação qualitativa do sinal óptico e do comportamento das curvas.

Percebe-se que a aplicação de atenuação, atraso ou até uma combinação destas duas variáveis nas fatias espectrais aumenta BER_D à medida que há um aumento na distância de propagação do sinal óptico.

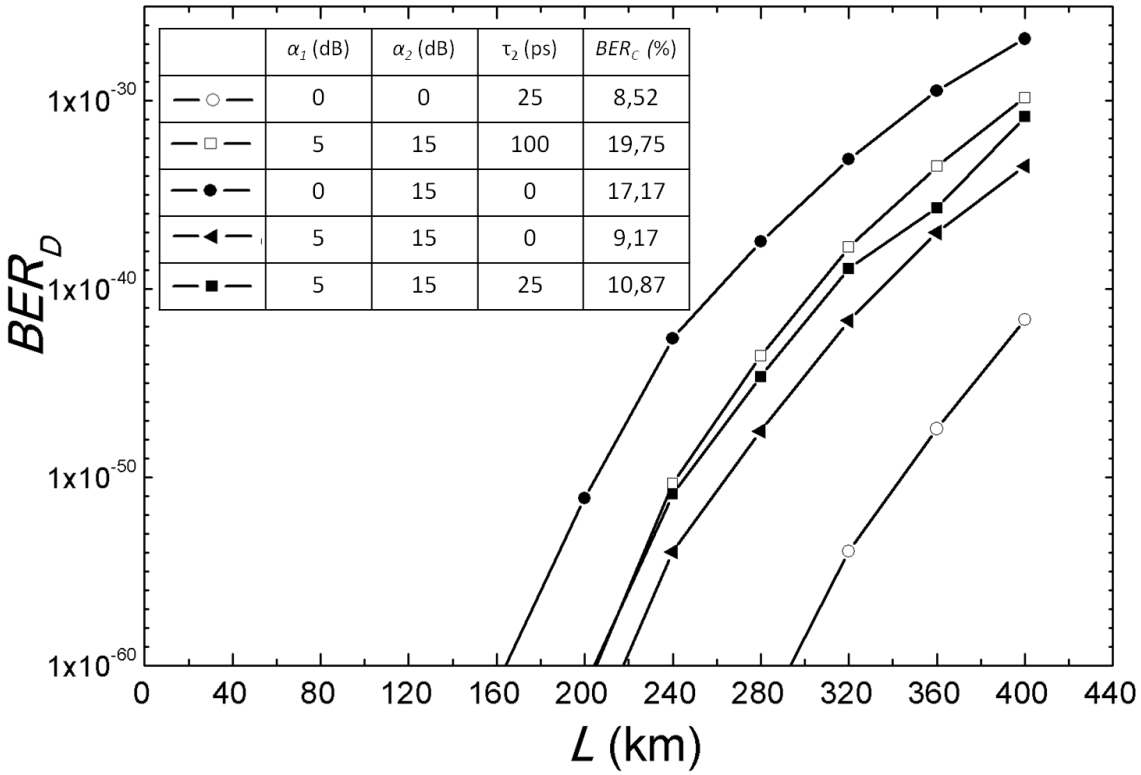


Fig. 14 – Sinal NRZ-OOK. Variação da BER_D em função da propagação dos sinais codificados. Apresentação relativa dos níveis de BER_D.

4.1.5. Influência do número de fatias espectrais na BER

A Fig. 15 ilustra a influência do número de fatias espectrais na BER_C. Foram comparados os resultados dos testes (ver diagrama de blocos apresentado na Fig. 6) de atenuação na fatia espectral central para três (40 GHz cada) e cinco

(24 GHz cada) fatias espectrais, totalizando, nos dois casos, um espectro óptico de 120 GHz.

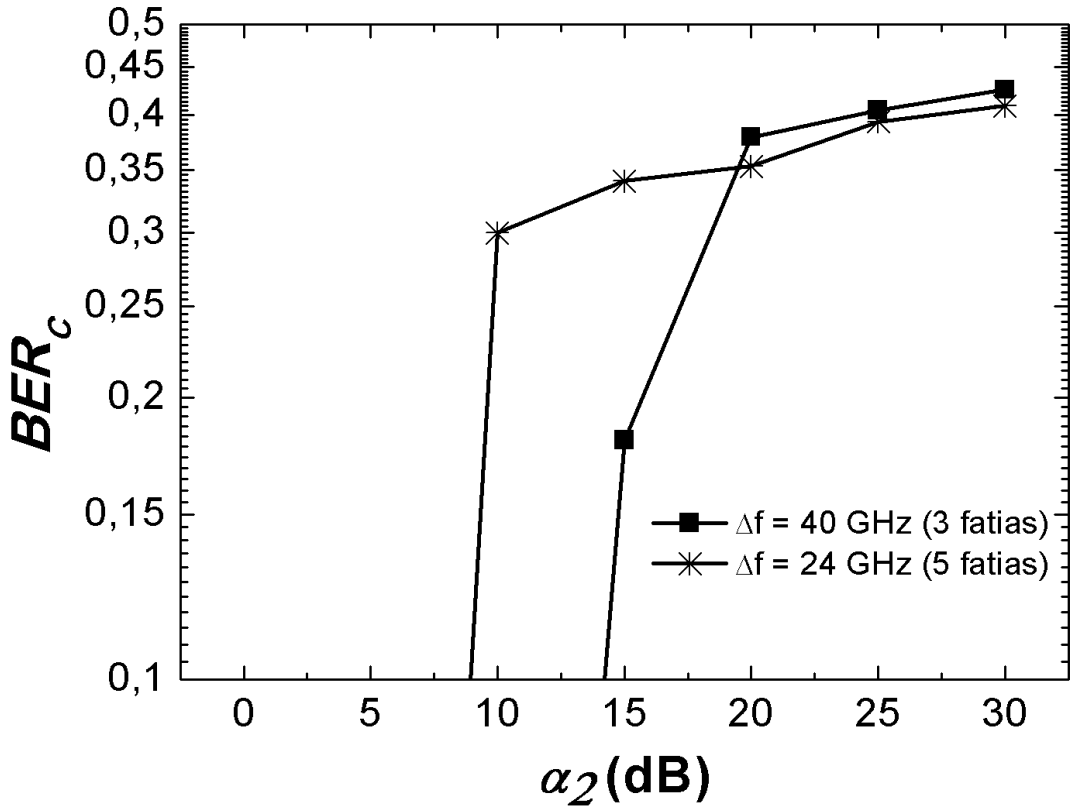


Fig. 15 – Sinal NRZ-OOK. Influência do número de fatias espectrais na BER_C

Verifica-se que o aumento do número de fatias incrementa a BER_C até $\alpha_2 \leq$ 20 dB. A partir deste valor, os dois casos apresentam um valor muito próximo de BER_C, com um desempenho ligeiramente superior para o codificador de apenas três filtros. É importante destacar que, para os dois casos, o sinal recuperado é idealmente livre de erros ($BER_D < 10^{-15}$).

4.2. Sinais DQPSK

A modulação de deslocamento de fase em quadratura (*Quadratura Phase Shift Keying*, QPSK), é uma técnica de modulação na qual é utilizada a fase para modular o sinal de informação. Através do deslocamento de fase do sinal (0, π, π/2 ou -π/2) é possível transmitir dois bits por símbolo. Abritrou-se as variações de fase de 0 e π correspondem aos valores do sinal do eixo em fase I (*In phase*, I) e as variações π/2 e -π/2 correspondem aos aos valores do sinal do eixo em quadratura Q (*Quadrature*, Q).

Os sinais DQPSK são uma variação da modulação QPSK. Possuem um formato de modulação de fase multinível, que a cada símbolo (2 bits) transmitido, aplica uma variação da fase em relação à fase atual do sinal, conforme tabela abaixo:

Dibit	Variação da fase em relação à fase atual
00	0
01	π/2
11	Π
10	- π/2

Como cada símbolo transmitido carrega dois bits, a largura de banda requerida para a transmissão de dados é reduzida à metade, implicando em uma eficiência espectral (SILVEIRA, 2009) que é o dobro daquela dos sinais NRZ-

OOK. Este é um dos motivos pelo qual a modulação DQPSK está sendo implementada comercialmente, sobretudo em sistemas WDM de 40 e 100 Gb/s.

4.2.1. Análises Espectral e Temporal

Para ilustrar os efeitos da técnica na modulação DQPSK, os espectros ópticos dos sinais (a) na entrada do codificador, (b) na saída do codificador e (c) na saída do decodificador são apresentados na Fig. 16. (ver diagrama de blocos apresentado na Fig. 6). Nela observa-se a portadora do sinal centrada em 193.1 THz e componentes espectrais mais significativas do sinal espaçadas da portadora em múltiplos de 20 GHz. Nota-se ainda que há uma grande proximidade no nível quantitativo da amplitude das componentes espectrais mais significantes espaçadas até 40 GHz da freqüência central.

Nessa mesma figura (Fig. 16), podemos observar o espectro óptico do sinal na saída do codificador (b). Nota-se o sinal óptico já fatiado, neste caso com atenuações de $\alpha_1 = 5$ dB, $\alpha_2 = 20$ dB e $\alpha_3 = 0$ dB, e atrasos $\tau_1 = \tau_2 = \tau_3 = 0$ ps, muito embora, através do espectro óptico, os atrasos não possam ser indicados. A largura de banda de cada fatia espectral é de 20 GHz.

A aplicação dos filtros de perfil retangular causa as variações abruptas nas transições das fatias espectrais e também elimina todo o sinal óptico que está fora da faixa de 193.07 e 193.13 THz. Já o espectro óptico do sinal recuperado na saída do decodificador é ilustrado em (c), considerando o mesmo diagrama de blocos da Fig. 6. Da mesma forma que a figura anterior, o sinal óptico que se encontra fora da faixa de 193.07 e 193.13 THz foi eliminado dada a aplicação dos

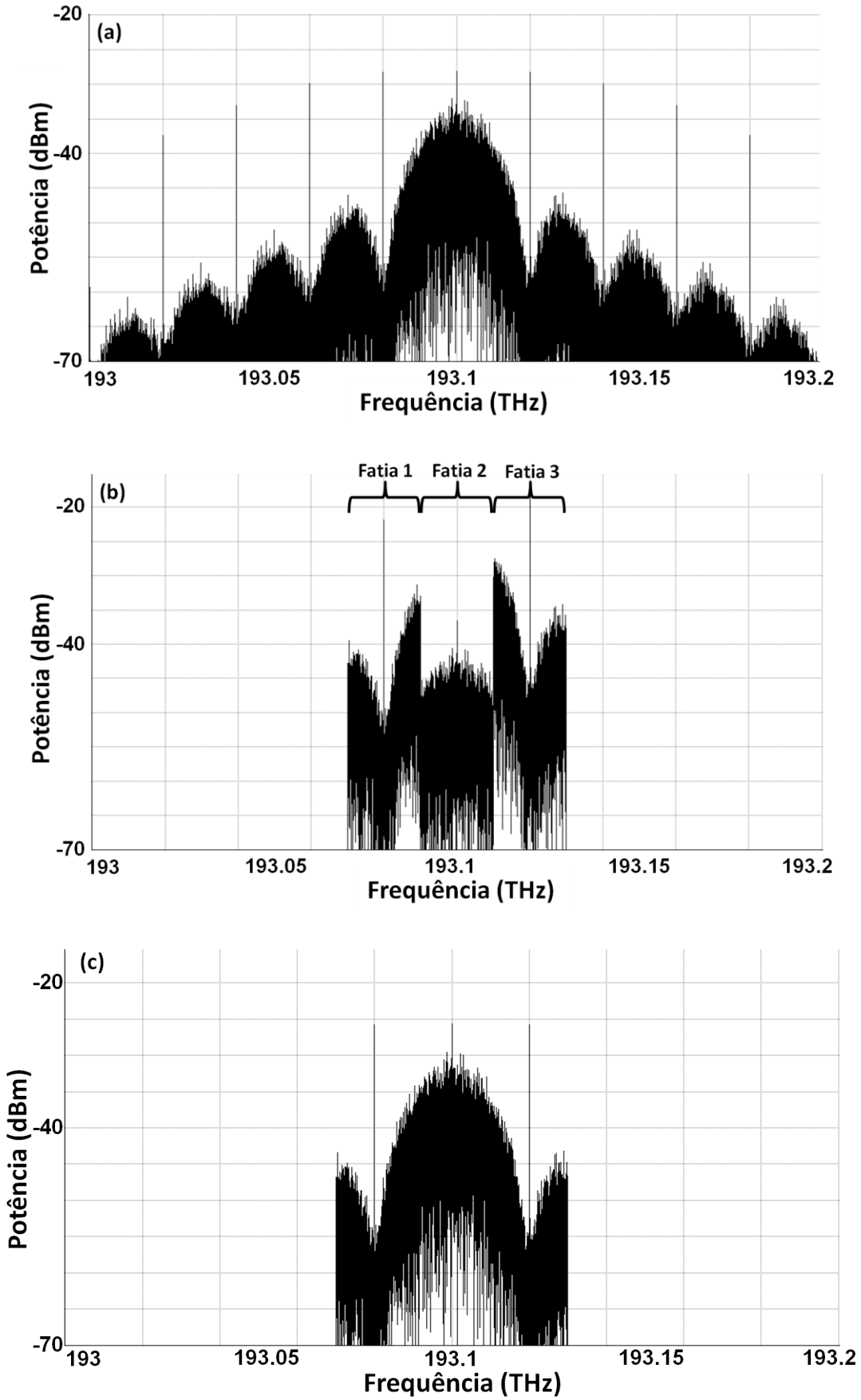


Fig. 16 – Sinal DQPSK. Espectro Óptico (a) na entrada do codificador; (b) na saída do codificador, para $\alpha_1 = 5$, $\alpha_2 = 20$ e $\alpha_3 = 0$ dB; $\tau_1 = \tau_2 = \tau_3 = 0$ ps.; e (c) na saída do codificador.

filtros nos blocos de codificação e decodificação. Entretanto, observa-se que dentro desta faixa de frequências, o sinal é muito próximo àquele apresentado no espectro do sinal original (a). As supressões das componentes laterais do espectro não impactam na qualidade do sinal verificado na saída do decodificador, uma vez que suas amplitudes não possuem valores expressivos.

De fato, as simulações indicam que este sinal possui BER_D inferior a 10^{-15} e pode, portanto, ser considerado livre de erros.

Os diagramas de olho relativos ao sinal óptico gerado nos eixos Q e I para os sinais (a) na entrada do codificador, (b) na saída do codificador e (c) na saída do decodificador, numa sequência pseudoaleatória de 2048 bits, são ilustrados na Fig. 17. Neste estudo, foram aplicadas atenuações de α_1 = 5 dB, α_2 = 20 dB e α_3 = 0 dB e atrasos $\tau_1 = \tau_2 = \tau_3 = 0$ ps. Conforme esperado, o diagrama de olho do sinal codificado (b) apresenta-se fechado e ininteligível, enquanto o diagrama de olho do sinal decodificado (c) apresenta-se aberto e com uma boa definição, o que implica em considerarmos que este sinal livre de erros, pois sua BER_D é inferior a 10^{-15}.

A ação da técnica proposta no domínio do tempo, para o sinal DQPSK é analisada na Fig. 18. Para evidenciarmos a eficácia da técnica, avaliamos uma sequência aleatória de 23 bits pré-definidos, que são propagados através dos eixos Q e I, utilizando-se o mesmo diagrama de blocos da Fig. 6, relativa aos sinais de entrada, codificado e decodificado, nas mesmas condições de atenuação e atraso apresentados no exemplo anterior. No eixo I, observa-se que o primeiro *slot* de bit (representado por *x*) não faz parte da sequência aleatória escolhida e refere-se ao período de bit relativo ao tempo de espera para disparo do primeiro bit naquele eixo.

Esta mesma figura (Fig. 18) ilustra a sequência temporal dos bits (a) na entrada do codificador, (b) na saída do codificador e (c) na saída do decodificador.

É possível verificar que o período de duração de cada bit é de 50 ps e que os níveis alto e baixo do sinal na entrada do codificador (a) são bem definidos. Após a codificação (b) observa-se uma versão bem distorcida do sinal de entrada do codificador. É possível identificar 7 bits errados (destacados na figura) com relação ao sinal de entrada (a), o que significa uma BER_C estimada de 26%,

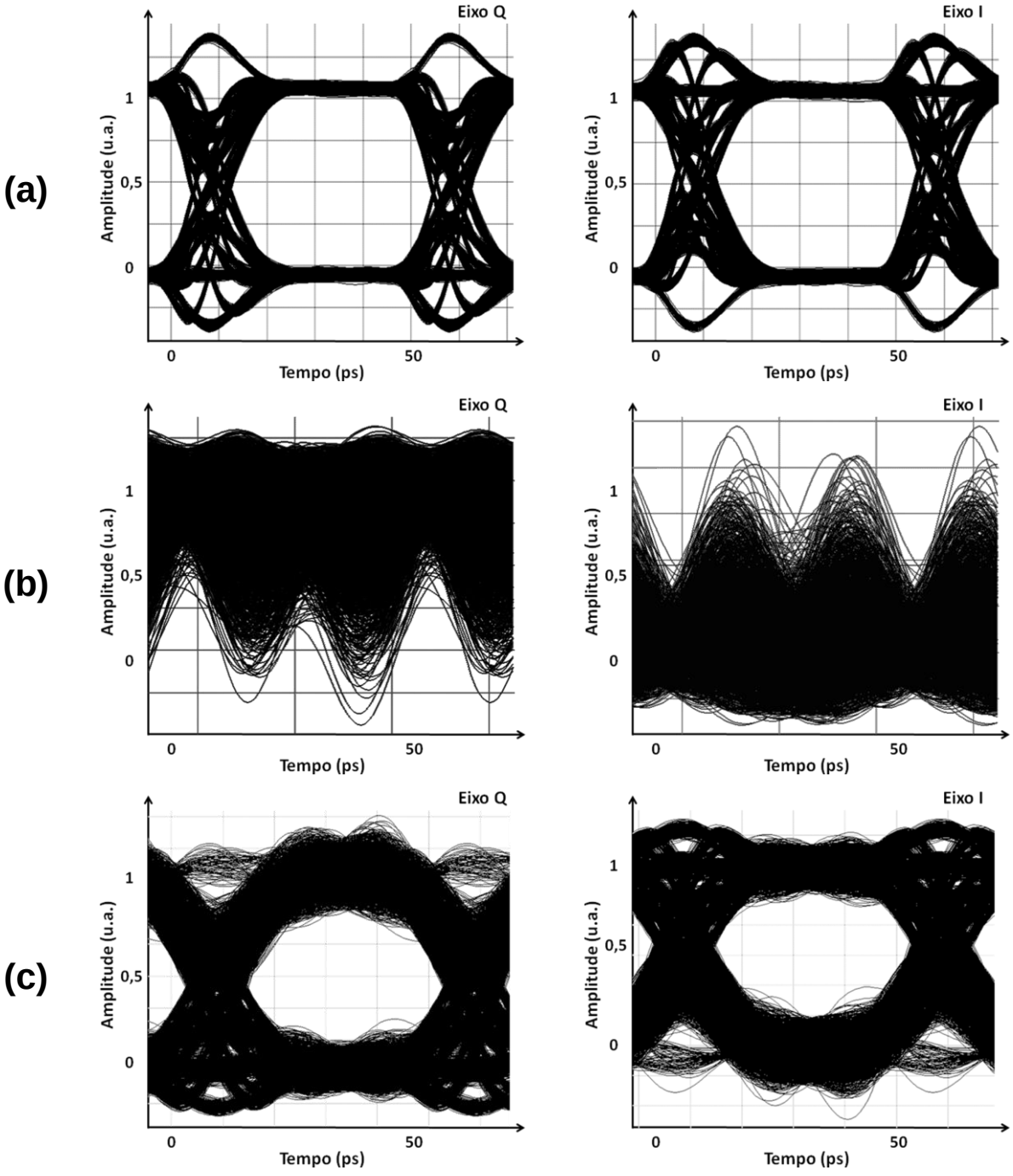


Fig. 17 – Sinal DQPSK. Sequência de Bits do sinal (a) na entrada do codificador, (b) codificado e (c) decodificado, para α_1 = 5, α_2 = 20 e α_3 = 0 dB; $\tau_1 = \tau_2 = \tau_3$ = 0 ps, nos Eixos Q e I.

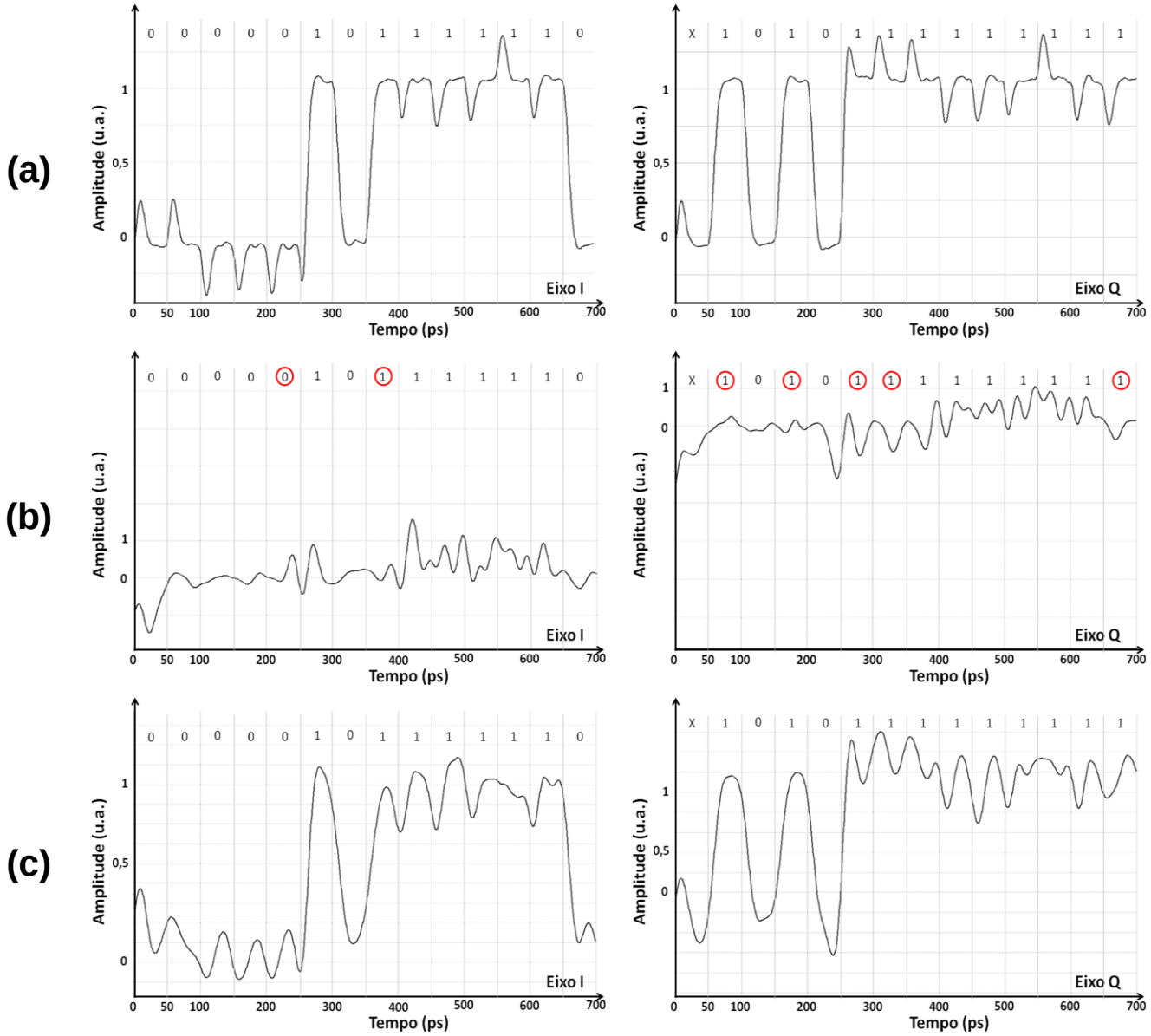


Fig. 18 – Sinal DQPSK. Sequencia de bits do sinal (a) na entrada do codificador, (b) codificado e (c) decodificado, para $\alpha_1 = 5$, $\alpha_2 = 20$ e $\alpha_3 = 0$ dB; $\tau_1 = \tau_2 = \tau_3 = 0$ ps, nos eixos Q e I.

considerando os 27 bits aleatórios gerados. Este número é semelhante à BER_C estimada quando se expande esta simulação para uma sequência aleatória de 2048 bits (25%). Já o sinal decodificado (c), mesmo não apresentando uma forma aproximada do sinal de entrada, mantém os níveis altos e baixos do sinal bem definidos. O sinal recuperado possui uma boa qualidade. Estes resultados tem caráter ilustrativo apenas. Como será visto a seguir, em várias situações é possível obter BER_D inferior a 10^{-15}.

4.2.2. Influência da Atenuação das Fatias Espectrais na BER

Na Fig. 19, apresentamos os resultados dos testes que avaliaram a variação da BER_D em função da aplicação da atenuação à fatia espectral central, combinadas com atenuações nas fatias espectrais laterais, para as seguintes situações:

a) $\alpha_1 = 0$ dB; $\alpha_3 = 5$ dB
b) $\alpha_1 = \alpha_3 = 0$ dB e
c) $\alpha_1 = 5$ dB; $\alpha_3 = 0$ dB.

BER_C é incrementada em função do aumento da atenuação na fatia central α_2, tendo um aumento expressivo à medida que há um crescimento de α_2, e assume um comportamento assintótico para $\alpha_2 \geq 20$ dB. Também se destaca a simetria que há entre as situações (a) e (c), relativas às atenuações nas fatias laterais α_1 e α_3, devido a simetria entre as fatias espectrais 1 e 3.

Por fim, é possível verificar que a atenuação nas fatias laterais, combinadas com a atenuação $\alpha_2 \leq 20$ dB implicam BER_C inferior àquela das atenuações aplicadas apenas à fatia central α_2. Isto se deve ao fato de que, nesta situação, há uma redução na diferença de potências entre as fatias espectrais central e lateral, causando, portanto, uma menor degradação do espectro óptico do sinal. Quando $\alpha_2 > 20$ dB, verifica-se que os resultados obtidos nas curvas são quantitativamente muito próximos.

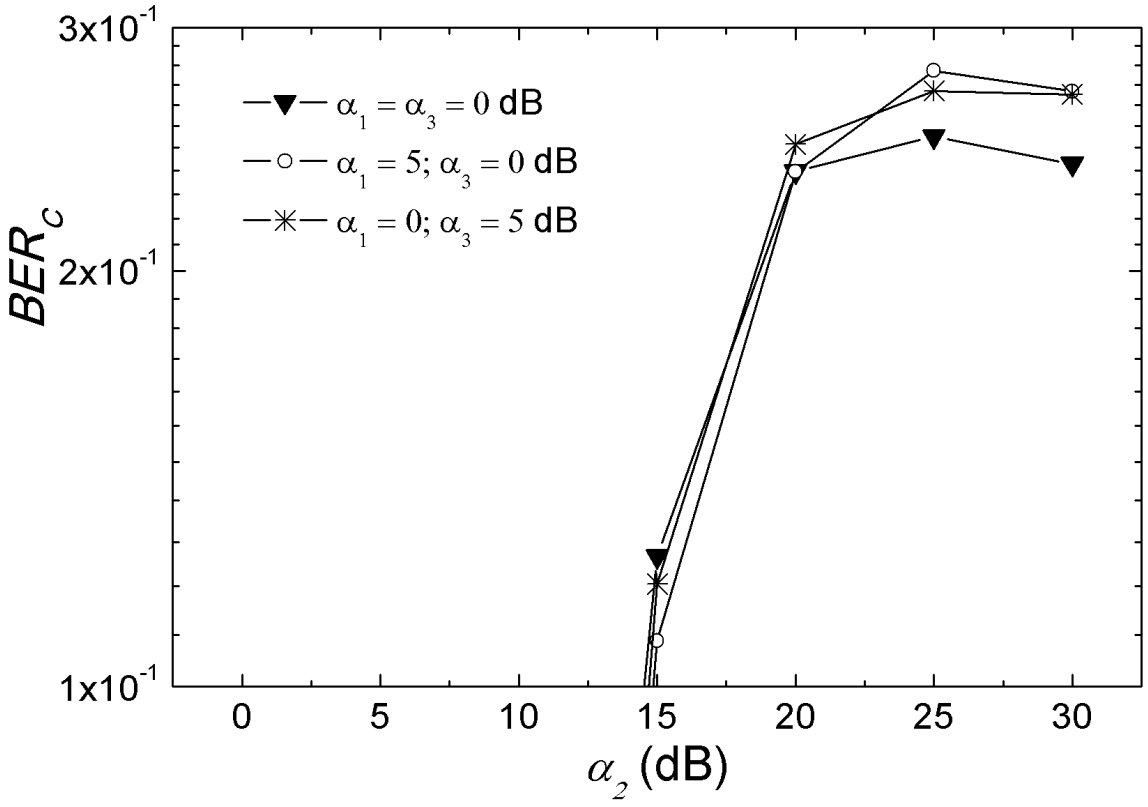


Fig. 19 – Sinal DQPSK. Dependência entre a BER_C do sinal codificado e α_2 para diferentes atenuações das fatias α_1 e α_3.

4.2.3. Influência do Atraso das Fatias Espectrais na BER

A Fig. 20 mostra a variação de BER_C em função da aplicação do atraso nas fatias espectrais central e laterais, para $\alpha_1 = \alpha_2 = \alpha_3 = 0$ dB, nos seguintes casos:

a) $\tau_1 = \tau_3 = 0$ ps, τ_2 variando;

b) $\tau_2 = \tau_3 = 0$ ps, τ_1 variando e

c) $\tau_1 = \tau_2 = 0$ ps, τ_3 variando.

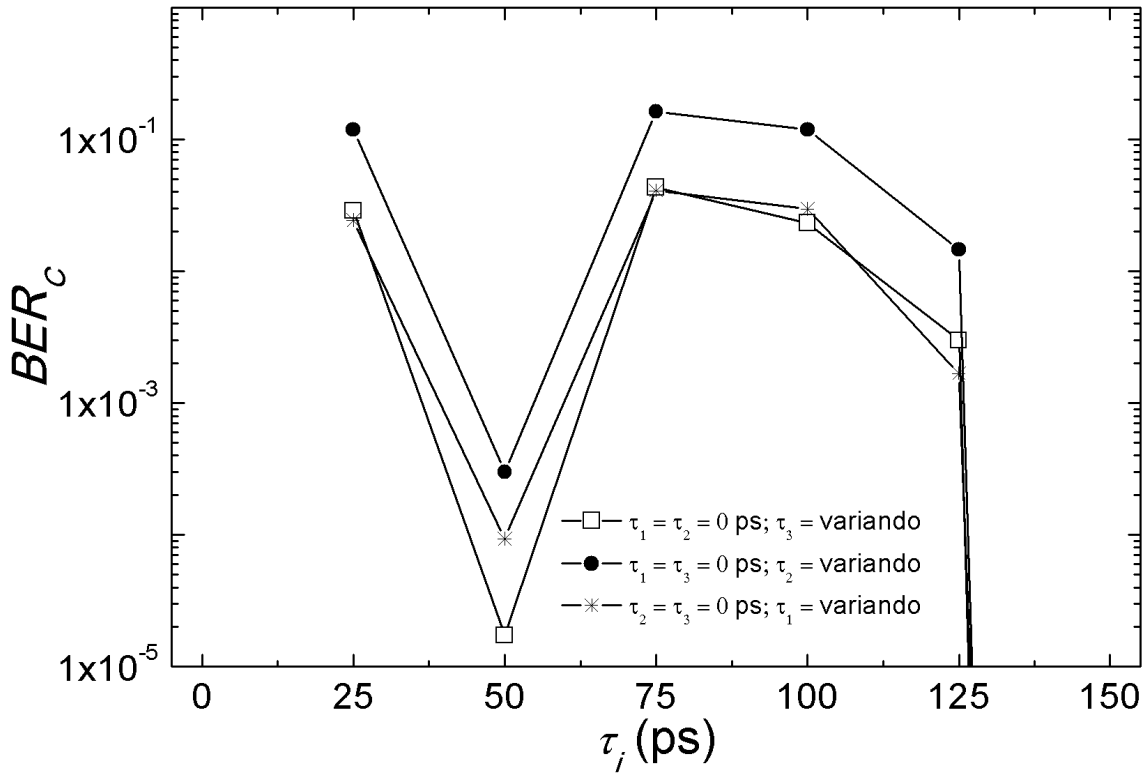


Fig. 20 – Sinal DQPSK. BER_C em função do incremento de τ_1, τ_2 e τ_3.

Observa-se que o comportamento de BER_C em função de τ_i não é monotônico. Isto sugere que os valores de τ_i devem ser criteriosamente escolhidos pois, podem conduzir a valores de BER_C maiores que 10% ou a outros valores inferiores a 10^{-5}. Estes resultados são qualitativa e quantitativamente distintos daqueles observados na Fig. 13 para sinais NRZ-OOK. Provavelmente, tal diferença está relacionada com o fato de atrasos implicarem em um desvio de fase e, portanto, terem um impacto maior sobre a codificação DQPSK.

Outro fato já citado anteriormente é aqui verificado. A simetria das fatias espectrais 1 e 3, causa uma sobreposição relativa das curvas dos atrasos τ_1 e τ_3, referentes às situações (b) e (c) devido a semelhança dos seus resultados quantitativos e a suas localizações em relação à frequência da portadora do sinal. Também, o incremento da BER_C em função da aplicação do atraso nas fatias espectrais laterais (situações (b) e (c)) são menos significativos quando

comparados aos resultados obtidos na aplicação dos mesmos atrasos na fatia central (situação (a)). Entretanto, quando são aplicadas atenuações simultaneamente a uma fatia espectral já atrasada, verifica-se um incremento significativo na grandeza da BER_C, o que nos leva a concluir que sinal é mais susceptível a variações de atenuação a atraso.

4.2.4. Propagação dos Sinais Codificados

Os testes foram realizados com até 10 enlaces de 40 km cada, no mesmo cenário de testes do diagrama de blocos apresentado na Fig. 6. Na Fig. 21, nota-se que a aplicação de atenuação, atraso ou até uma combinação destas duas variáveis nas fatias espectrais aumenta a BER_D à medida que há um aumento na distância de propagação do sinal óptico. Na situação em que α_2 = 15 dB, obtém-se no decodificador o sinal recuperado com uma $BER_D = 10^{-6}$, para um enlace com L = 400 km. Esta é a pior situação, do ponto de vista da qualidade do sinal recuperado na saída do decodificador.

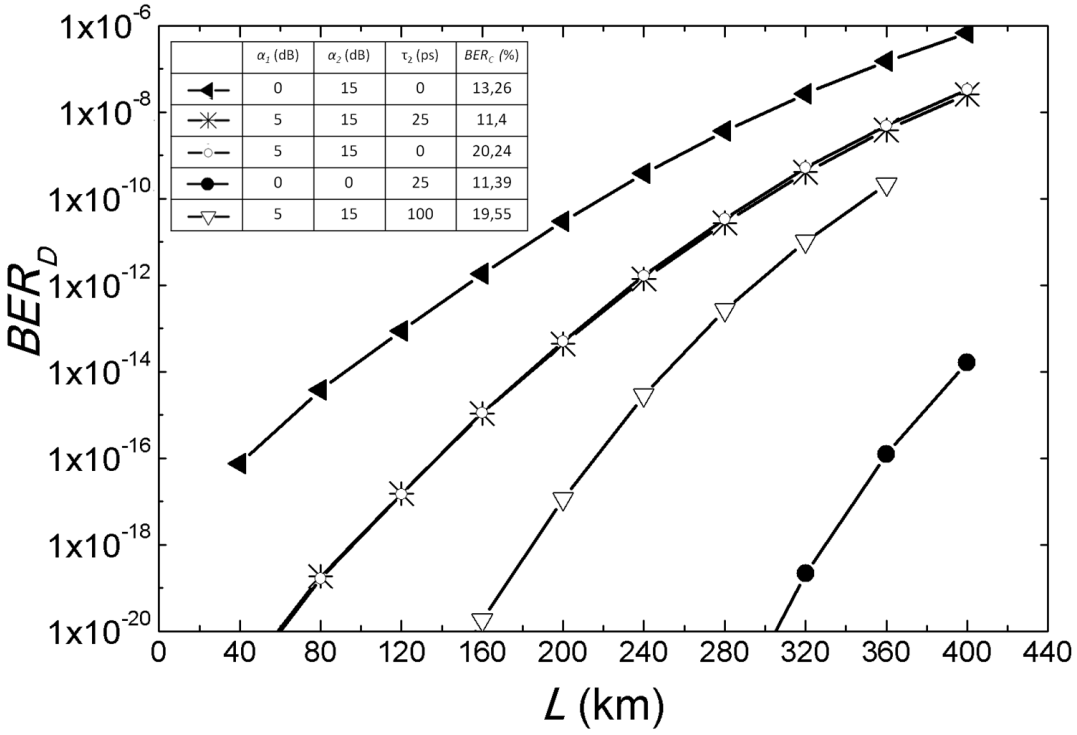


Fig. 21 – Sinal DQPSK. Variação da BER_D em função da propagação dos sinais codificados. Apresentação relativa dos níveis de BER_D.

4.3. Impacto da redução da largura de banda das fatias espectrais no desempenho dos sinais

Nas seções anteriores, apresentamos os resultados obtidos das simulações de rede para os sinais NRZ-OOK e DQPSK, nos quais a largura de cada fatia espectral (Δf) era, respectivamente, de 40 e 20 GHz. A seguir, faremos a análise do impacto da redução da largura total de banda dessas fatias espectrais, considerando que Δf = 16.5 GHz, para qualquer uma das modulações analisadas.

A Fig. 22 apresenta o incremento de BER_C devido à redução da largura de cada fatia espectral (Δf), para a modulação NRZ-OOK. As situações avaliadas estão abaixo relacionadas:

a) $\alpha_2 = 15$ dB
b) $\alpha_1 = 5$ dB; $\alpha_2 = 15$ dB e
c) $\alpha_1 = 5$ dB; $\alpha_2 = 15$ dB; $\tau_2 = 25$ ps

Verifica-se que a redução de Δf provoca um incremento mais efetivo de BER_C nas situações (a) e (b), do que na situação (c), quando não há a aplicação do atraso.

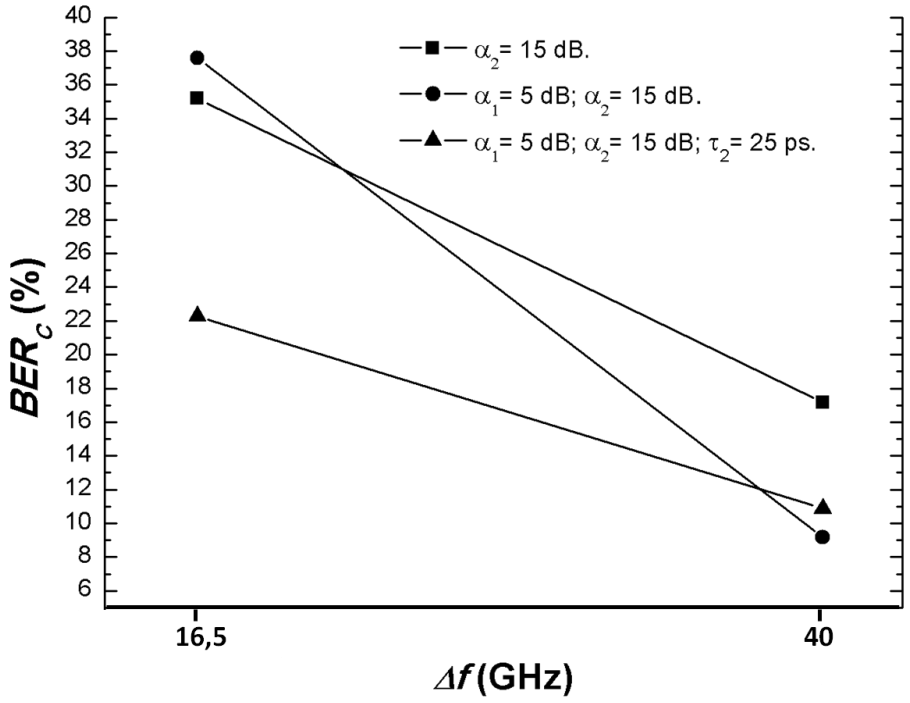


Fig. 22 – Sinal NRZ-OOK. Incremento de BER_C devido a redução da largura das fatias espectrais.

O gráfico da Fig. 23 compara os resultados obtidos nas simulações para o sinal NRZ-OOK com fatias espectrais (Δf) de 40 GHz e 16.5 GHz, com até 10

enlaces de 40 km cada, no mesmo cenário de testes do diagrama de blocos apresentado na Fig. 6. As situações avaliadas foram as mesmas citadas anteriormente e é apresentado (de maneira relativa) os resultados obtidos de BER_D, para possibilitar uma comparação qualitativa do sinal óptico.

Como já havíamos analisado na seção 4.1.4, em todas estas situações onde Δf = 40 GHz, é possível obter no decodificador o sinal recuperado e idealmente livre de erros, com $BER_D < 10^{-15}$. Verifica-se que há um incremento da BER_D quando a largura de banda é reduzida a Δf = 16.5 GHz, para qualquer um dos casos. Este incremento ocorre porque as componentes espectrais que estão fora da banda entre 193.07525 e 193.12475 THz são eliminadas, em função da aplicação dos filtros de perfil retangular, já discutidas anteriormente. A BER_D cresce com o aumento do comprimento dos enlaces. Nota-se também que o sinal óptico é recuperado praticamente livre de erro ($BER_D < 10^{-15}$) até L = 120 km para qualquer uma das situações avaliadas e que BER_D é da ordem de 10^{-6} na situação (a) quando L = 400 km, relativo a 10 enlaces. Nestes casos, conforme citado na Seção 3.1, poderia ser aplicado o recurso da correção antecipada de erros, FEC.

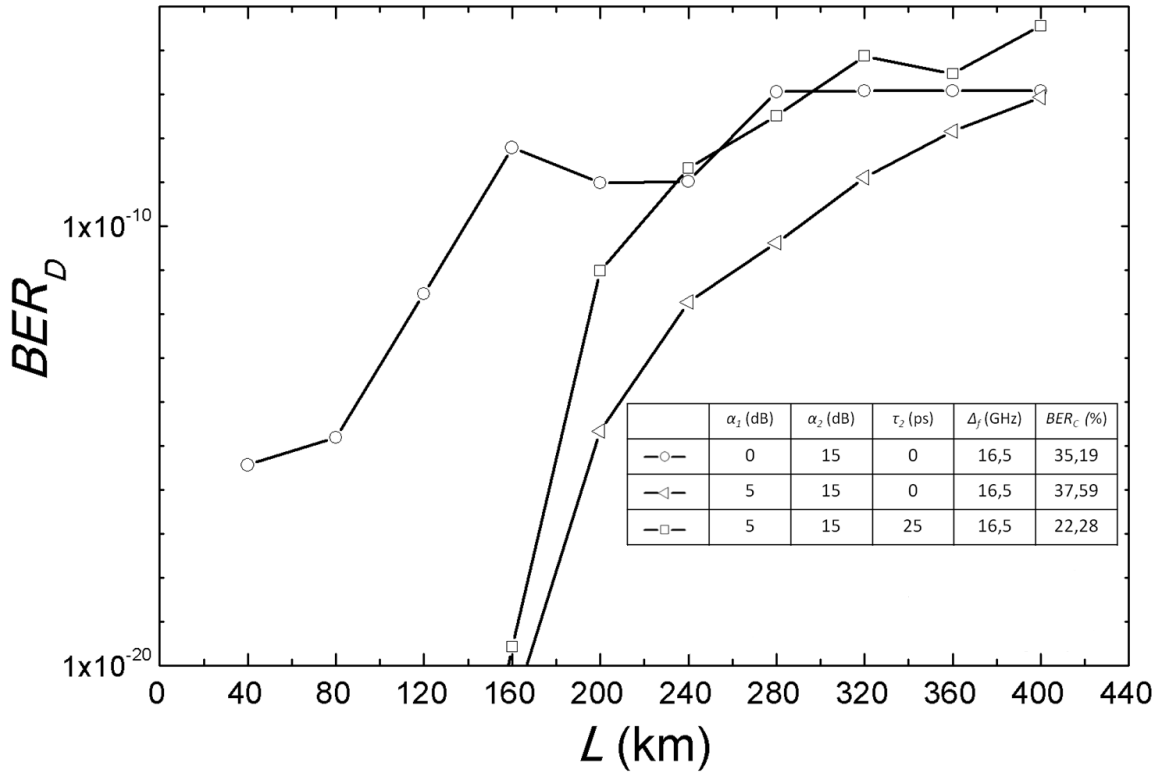


Fig. 23 – Sinal NRZ-OOK. Incremento de BER_D em função da redução da fatia espectral.

Analogamente ao apresentado nas duas figuras anteriores, as Figs. 24 e 25 ilustram, respectivamente, o incremento de BER_C devido à redução da largura de cada fatia espectral (Δf), para a modulação DQPSK, e à comparação dos resultados obtidos nas simulações para o sinal DQPSK com fatias espectrais (Δf) de 20 GHz e 16.5 GHz. Da mesma forma, as simulações utilizaram o mesmo cenário de testes do diagrama de blocos apresentado na Fig. 6, com até 10 enlaces de 40 km cada. Foram avaliadas as situações a seguir:

a) $\alpha_2 = 15$ dB
b) $\alpha_1 = 5$ dB; $\alpha_2 = 15$ dB e
c) $\alpha_1 = 5$ dB; $\alpha_2 = 15$ dB; $\tau_2 = 25$ ps.

Na Fig. 24, verifica-se que a redução da largura fatia espectral tem um impacto pouco relevante no incremento da BER_C, pois estas fatias espectrais

possuem valores absolutos muito próximos. Da mesma forma, como era de se esperar, a redução da largura da fatia espectral causa um incremento na BER_D (Fig. 25). Nesse novo cenário (Δf = 16.5 GHz), os resultados mostraram que a BER_D têm um aumento pouco significativo e, em simulações realizadas para a pior situação (a), notou-se que a BER_D atingiu valores da ordem de grandeza de 10^{-6}, em comparação à grandeza de 10^{-7} em que Δf = 20 GHz, num enlace de 400 km. Da mesma forma, conforme citado na Seção 3.1, é possível a aplicação da correção antecipada de erros, FEC para a recuperação da qualidade do sinal.

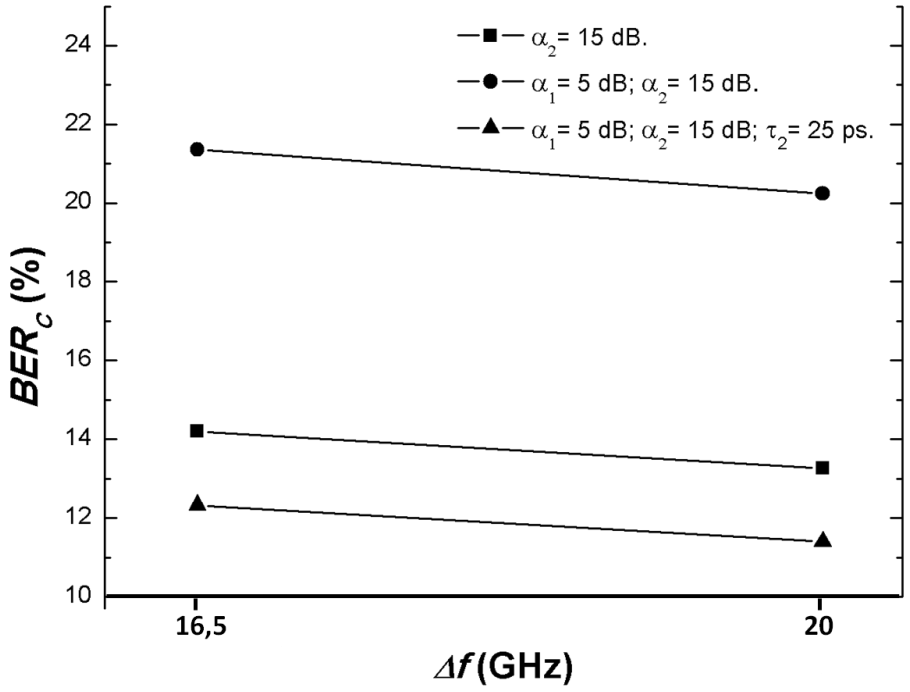
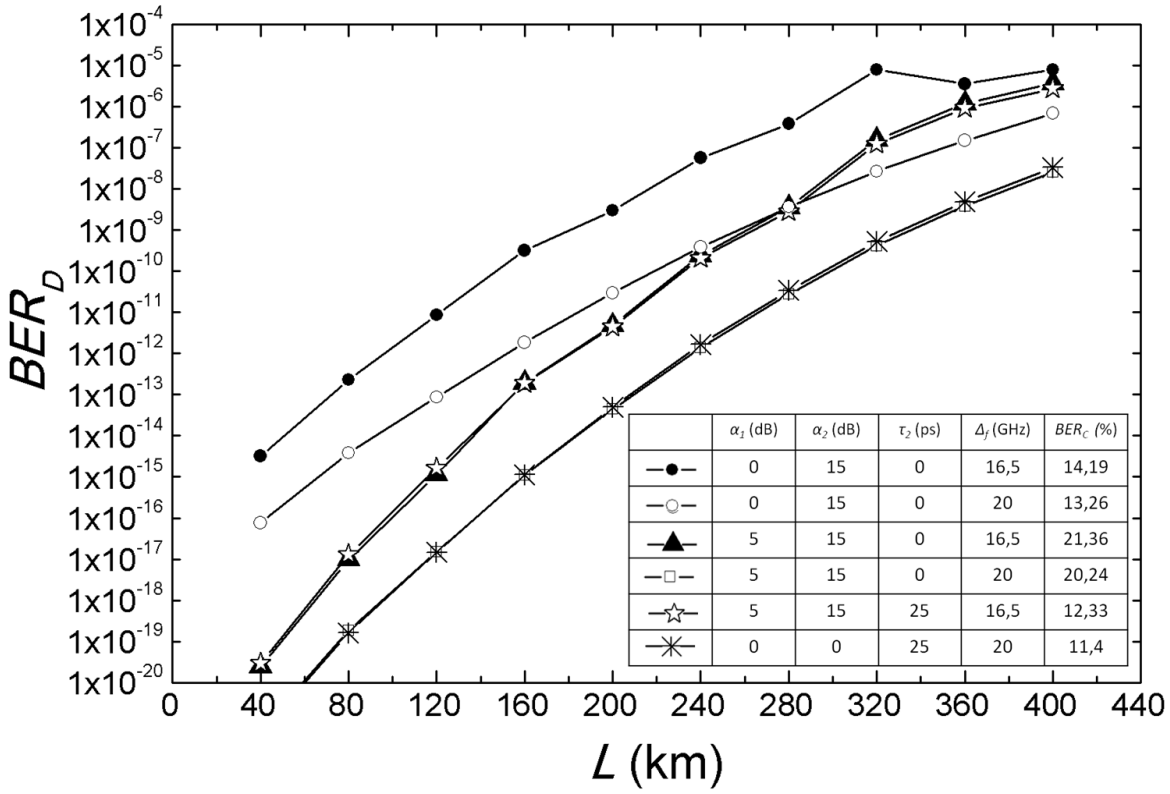


Fig. 24 - Sinal DQPSK. Penalidade aplicada à BER_C devido a redução da largura das fatias espectrais.

4.4. Comparação dos Resultados dos Sinais NRZ-OOK e DQPSK



	α_1 (dB)	α_2 (dB)	τ_2 (ps)	Δ_f (GHz)	BER_C (%)
—●—	0	15	0	16,5	14,19
—○—	0	15	0	20	13,26
—▲—	5	15	0	16,5	21,36
—□—	5	15	0	20	20,24
—☆—	5	15	25	16,5	12,33
—✳—	0	0	25	20	11,4

Fig. 25 – Sinal DQPSK. Incremento de BER_D em função da redução da fatia espectral.

Nas seções anteriores, verificamos que há uma maior eficiência na criptografia do sinal quando se aplicam alterações na fatia espectral central, já que as alterações nas fatias espectrais laterais são menos impactantes à BER. Em função disto, a comparação dos resultados obtidos durante as simulações de rede levarão em conta as alterações na fatia central do espectro óptico dos dois sinais ópticos estudados nesse trabalho.

Na Fig. 26, mostramos os resultados dos testes que avaliaram a variação da BER_C em função da aplicação da atenuação a fatia espectral central, para as seguintes situações:

a) $\alpha_1 = \alpha_3 = 0$ dB
b) $\alpha_1 = 0$ dB; $\alpha_3 = 5$ dB.

Observa-se na figura que o sinal NRZ-OOK apresenta maior sensibilidade à aplicação de baixas atenuações (até 15 dB) do que o sinal DQPSK. Também, o sinal NRZ-OOK, apresenta uma BER_C mais elevada quando as atenuações são superiores a 15 dB.

A sensibilidade à aplicação de atraso na fatia espectral central, combinadas com a aplicação de atenuações nas fatias espectrais 1 e 2 é apresentada na Fig. 27. Observa-se que o sinal NRZ-OOK apresenta BER_C mais elevada quando é aplicada uma atenuação maior na fatia espectral central, quando comparado ao sinal DQPSK, apesar de que, qualitativamente, os resultados são muito próximos.

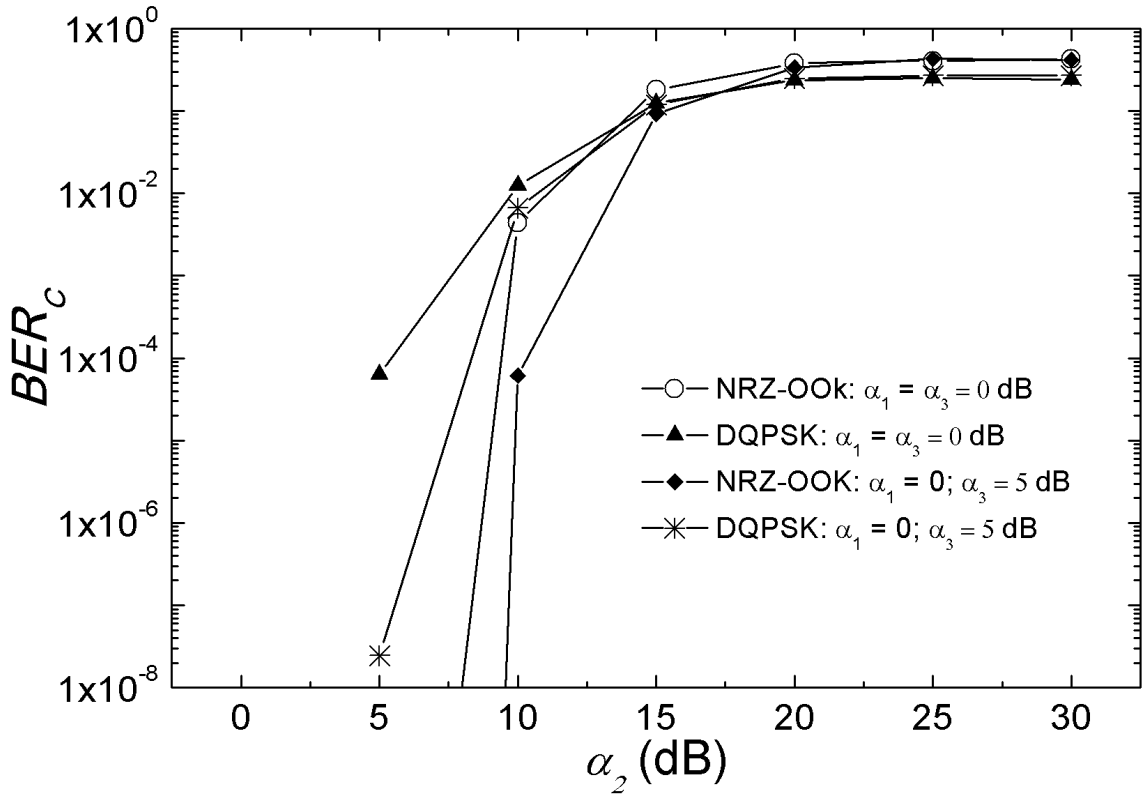


Fig. 26 – Comparação dos sinais NRZ-OOK e DQPSK. Dependência entre a BER_C e α_2.

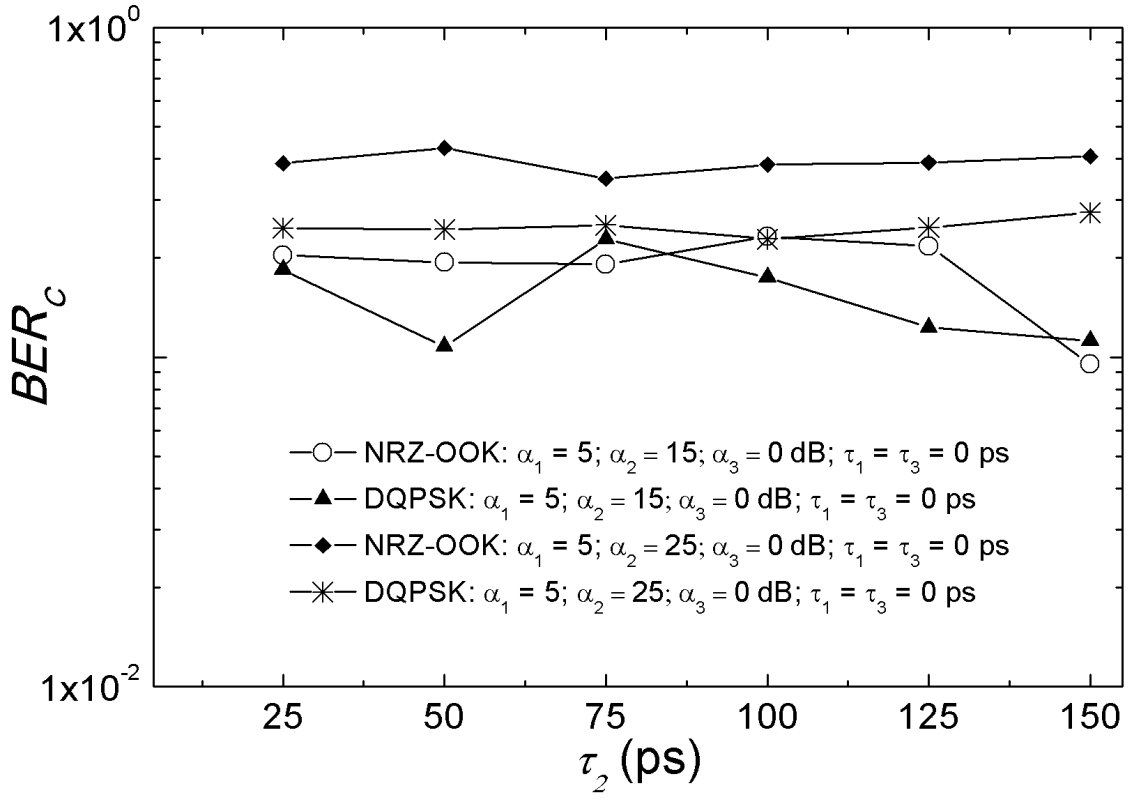


Fig. 27 – Comparação dos Sinais NRZ-OOK e DQPSK em função do incremento de τ_2.

No próximo capítulo, serão apresentadas as conclusões e considerações finais deste estudo, com base nos resultados das simulações aqui apresentadas.

5. CONCLUSÕES

No Capítulo 4, apresentaram-se os resultados obtidos durante as simulações para sinais NRZ-OOK e DQPSK de 40 Gbps. Em particular, foi considerada para cada um destes sinais as análises espectral e temporal do sinal óptico, incluindo a influência que o atraso e a atenuação das fatias espectrais causam à BER. Analisou-se também a influência da BER quando o sinal é propagado por enlaces de 40 km, até o limite de 10 enlaces e, por fim, qual o impacto da redução da largura de banda das fatias espectrais no desempenho dos sinais. Neste capítulo, apresenta-se as conclusões acerca dos resultados obtidos através das simulações e as perspectivas de continuidade das pesquisas sobre o tema.

O estudo propôs uma técnica inovadora para criptografia totalmente óptica de sinais NRZ-OOK e DQPSK em redes óticas totalmente transparentes. A técnica é baseada na divisão de um sinal óptico em *n* fatias espectrais que, posteriormente, são submetidas a atenuações e atrasos próprios para codificação e decodificação do sinal transmitido.

Para simplificar a avaliação da influência das variações de α e τ no sinal óptico, foram inicialmente consideradas três fatias espectrais. Para a modulação NRZ-OOK, a largura de banda utilizada para cada fatia foi de 40 GHz, totalizando 120 GHz. Já na modulação DQPSK, foi utilizada uma banda total de 60 GHz, composta de três fatias de largura simétrica de 20 GHz.

A eficácia da técnica foi avaliada através da fotodetecção do sinal óptico nas saídas do codificador e decodificador com o objetivo de se avaliar a BER. Os resultados indicam que o sinal codificado atinge BER_C entre 9 e 42% para sinais NRZ-OOK e entre 11 e 24% para sinais DQPSK. Já o sinal decodificado, para a modulação NRZ-OOK, apresenta-se praticamente livre de erros ($BER_D < 10^{-15}$) e na modulação DQPSK a BER_D é inferior a 10^{-6}.

Durante o desenvolvimento deste trabalho, não foi considerada em nenhuma situação, a utilização de recursos correção antecipada de erros (*Foward Error Correction*, FEC). Muito embora este recurso possa alterar o limite máximo de propagação do sinal óptico, se a FEC for muito eficiente, o sinal poderá ser decodificado por um agente que esteja além do desejado. Desta forma, é importante que se mantenha um compromisso entre o alcance do limite de propagação que é ofertado pelo emprego deste recurso e o risco da recuperação deste sinal codificado de uma maneira não requerida.

Posteriormente, realizaram-se simulações que consideravam a redução da largura das fatias do espectro óptico para dentro do limite de banda de 50 GHz da grade de recomendação do ITU-T. Nesta situação, verificou-se que o sinal NRZ-OOK sofre maior degradação quando comparado ao sinal DQPSK. Neste ponto, é importante destacar que a redução de Δf no sinal NRZ-OOK foi muito mais significativa (de 40 para 16.5 GHz) do que para o sinal DQPSK (de 20 para 16.5 GHz), o que, certamente, é reflexo desta observação.

Tais resultados foram obtidos através de simulações de rede que consideraram ambientes onde o codificador e o decodificador utilizavam filtros de perfil retangular. Ambos estavam dispostos nas configurações *back-to-back*, e em ambientes de até dez enlaces de rede de 40 km cada. Neste caso, utilizaram-se as fibras compensadoras de dispersão. Cabe destaque que os resultados não

indicaram a influência do efeito de mistura de quatro ondas (*four wave mixing*, FWM) entre as componentes espectrais do sinal codificado.

Em relação a outras abordagens apresentadas na literatura, a técnica apresenta as seguintes vantagens:

a) não provê o alargamento espectral,

b) permite a alteração da chave criptográfica quando necessário,

c) permite o controle analógico da amplitude e do atraso nas fatias espectrais, e

d) a técnica proposta é, em princípio, transparente à taxa de transmissão e ao formato de modulação utilizados. Considerando o advento das altíssimas taxas de transmissão de dados, da ordem de 100 Gbps, que utilizam uma transmissão de sinais coerentes na modulação de dupla polarização por deslocamento de fase diferencial em quadratura (*Dual-Polarization Diferential Quadrature Phase Shift Keying,* DP-DQPSK), seria possível a aplicação de duas codificações simultâneas no sinal transmitido: um codificador DQPSK na polarização X e outro que poderia ser diferente na polarização Y. Neste contexto, torna-se desejável a continuidade dos estudos para outros tipos de modulação empregados para altas taxa de transmissão de dados, tais como a modulação em amplitude de quadratura (*Quadrature Amplitude Modulation*, QAM).

Dada a importância que a segurança da informação vem tomando dentro das Redes de Telecomunicações, e a necessidade cada vez maior de elevadas taxas de transmissão de dados, é desejável que este trabalho seja continuado a partir dos estudos da técnica aplicada à taxas de transmissão de 100 Gbps e 400 Gbps. Isto também é importante para o caso de continuidade de outro trabalho em desenvolvimento que leva em consideração a aplicação de filtros de perfil real nas mesmas condições apresentadas aqui (SILVA, 2012).

Por fim, também seria muito oportuna a execução de testes experimentais para comprovar a eficiência da técnica, com o objetivo de se determinar o grau de segurança que a chave criptográfica emprega aos sistemas. Estes testes poderiam ser realizados com elementos discretos (filtros, atenuadores e ODLs), com o referido Waveshaper ® e, até mesmo, com elementos integrados em fotônica de Silício. Além disso, a fim de reduzir a chance de um intruso descobrir a chave criptográfica utilizada, seria interessante verificar a pertinência da utilização de elementos que alterassem dinamicamente a atenuação (como os moduladores de intensidade) e o atraso de cada fatia espectral.

TRABALHOS PUBLICADOS

ABBADE, M.L.F.; FOSSALUZZA JR., L.A.; SILVA, R.F.; FAGOTTO, E.A.M. Criptografia Óptica Mediante Controle Analógico da Amplitude e do Atraso de Fatias Espectrais: Análise para Sinais NRZ. MOMAG, 2012. João Pessoa, PB, Brasil.

REFERÊNCIAS

ABBADE, M.L.F.; FOSSALUZZA JR., L.A.; SILVA, R.F.; FAGOTTO, E.A.M. Criptografia Óptica Mediante Controle Analógico da Amplitude e do Atraso de Fatias Espectrais: Análise para Sinais NRZ. MOMAG-2012, João Pessoa, PB, Brasil, 2012.

ABDALLAH, W.; HAMDI, M; BOUDRIGA, N. An All Optical Configurable and Secure OCDMA System Implementation Using Loop Based Optical Delay Lines. *IEEE, Icton,* 2011.

AGARWAL, A.; TOLIVER, P.; MENENDEZ, R.; ETEMAD, S.; JACKEL, J.; YOUNG, J.; BANWELL, T. LITTLE, B. E.; CHU, S. T.; CHEN, W.; CHEN, W.; HRYNIEWICZ, J.; JOHNSON, D. G.; KING, O.; DAVIDSON, R.; DONOVAN, K.; DELFYETT, P. J. Fully Programmable Ring-Resonator-Based Integrated Photonic Circuit Phase Coherent Applications. *Journal of Lightwave Technology*, vol. 24, nº 1, pp. 77-87, 2006.

BORGERTH, V. *Sox – Entendendo a Lei Sarbanes – Oxley*, Thompson, 1ª edição, 2006, 117 p.

CASTRO, J.; DJORDJEVIC, I.; GERAGHTY, D. Novel Super Structured Bragg Gratings for Optical Encryption. Journal of Lightwave Technology, vol. 24, nº 4, pp. 1875-1885, 2006.

CINCOTTI, G.; SACCHIERI, V.; MAZACCA, G.; KATAOKA, N.; WADA, N.; NAKAGAWA, N. KITAYAMA, K. I. Physical Layer Security: All-Optical Cryptography in Access Networks. IEEE, Icton, 2008.

CORNEJO, J. A.; PEREZ, C. E.; TOCNAYE, J. B. WDM – Compatible Channel Scrambling for Secure High-Data-Rate Optical Transmissions. *Journal of Lightwave Technology*, vol. 25, pp. 2081-2089, 2007.

ETEMAD, S.; ARGAWAL, A.; BANWELL, T.; JACKEL, J.; MENENDEZ, R.; TOLIVER, P. OCDM-based photonic layer “security” sacalable to 100 Gbits/s for existing WDM network. *Journal of Optical Networking*, vol. 6, Nº 7, pp.948-967, New Jersey, USA, 2007.

FALTA, K.; CAMERON, C. Balancing Performance, Flexibility and Scalability in Optical Networks. *Finisar Corporation*, Sunnyvale, California, USA, 2012. Em: <www.finisar.com>. Acesso em: 03 agosto 2012.

FOK, M. P.; PRUCNAL, P. R. All-Optical Encryption for Optical Network with Interleaved Waveband Switching Modulation. *OSA/OFC/NFOEC, Optical Society of America*, IEEE. 2009.

GERSTEL, O.; JINNO, M.; LORD, A.; BEN YOO. S. J. Elastic Optical Networking: A New Dawn for the Optical Layer?. *IEEE Communications Magazine*, pp. S12-S20, February 2012.

HARASAWA, K.; HIROTA, O.; YAMASHITA, K.; HONDA, M.; KENICHI, O. SHIGETO, A. TAKESHI, H. YOSHIFUMI, D. Quantum Encryption Communication Over 192-km 2.5-Gbit/s Line With Optical Transceivers Employing. *Journal of Lightwave Technology*, vol. 29, Nº 3, pp. 316-323, 2011.

HORST, F.; GREEN, W.M.J.; ASSEFA, S.; SHANK, S.M.; OFFREIN, B.J.; VLASOV, Y.A. WDM Filters for Silicon Photonics Transceivers. *The 16th Opto-Eletronics and Communications Conference OECC*, pp. 842-845, Kaohsiung, Taiwan, 2011.

HUISZOON, B.; AUGUSTIN, L.M.; HANFOUG, R.; BAKKER, L.; SANDER-JOCHEM, M. J. H.; FLEDDERUS, E. R.; KHOE, G. D.; VAN DER TOL, J. J. G. M.; WAARDT, H.; SMIT, M. K.; KOONEN, A. M. J. Integrated Parallel Spectral OCDMA En/Decoder. *IEEE, Photonics Technology Letters*, vol.19, no.7, pp. 528-530, 2007.

KAHN, D. The Codebreakers. *Macmillan*, 2nd Ed., 1.995.

KARTALOPOULOS, S. V. Security in Advanced Optical Communications Networks. *IEEE, ICC*, Oklahoma, 2009.

KITAYAMA, K. I.; SASAKI, M.; ARAKI, S.; TSUBOKAWA, M.; TOMITA, A.; INOUE, K.; HARASAWA, K.; NAGASAKO, Y.; TAKADA, A. Security in Photonic Networks: Threats and Security Enhancement. *Journal of Lightwave Technology*, vol. 29, pp. 3210-3222, 2011.

KOSTINSKI, N.; KRAVTSOV, K.; PRUCNAL, P. R. Demonstration of an All-Optical OCDMA Encryption and Decryption System With Variable Two-Code Keying. *IEEE Photonics Technology Letters*, vol. 20, no. 24, 2008.

LADD, T. D.; JELEZKO, F.; LAFLAMME, R.; NAKAMURA, Y.; MONROE, C.; O'BRIEN, J. L. Quantum computers. *Nature*, vol. 464, no. 7285, pp. 45-53, 2010.

PONEMOM INSTITUTE LLC. Research Department. **Fourth Annual US Cost of Data Breach Study**. Michigan USA, 2009. Em: <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf>. Acesso em: 25 setembro 2012..

PRUCNAL, P. R.; FOK, M. P.; DENG, Y.; WANG, Z. Physical layer security in fiber-optic netwoerks using optical signal processing. *SPIE-OSA-IEEE Asia Communications and Photonics*. 2009. Vol. 7632, pp. M1-1-M1-10.

RAMASWAMI, R.; SIVARAJAN, K.; SASAKI, G. Optical Networks: A Practical Perspective, *Morgan Kaufmann*, 3rd edition, 2009.

REIS JR., J.V. ***Modelagem de Redes CDMA-PON Baseadas em Técnicas de Cancelamento Paralelo e Código Corretores de Erros***. Dissertação de Mestrado. São Carlos:Universidade de São Paulo, 2009.

SANTOS FILHO, R.V.B. ***Análise de Sistemas CDMA Ópticos***. Dissertação de Mestrado. São Carlos: Universidade de São Paulo, 2006.

SHANEMAN, K. & GRAY, S. Optical Network Sevcurity: Technical Analysis of Fiber Tapping Mechanisms and Methods for Detection & Prevention. Milcon, 2004. *IEEE Military Communication Conference*, p. 711-717, New York, 2004.

SILVA, R.F. ***Análise de Criptografia óptica realizada mediante controle da amplitude e do atraso de fatias espectrais geradas com perfil de filtros ópticos comerciais.*** Dissertação de Mestrado. Campinas: Pontifícia Universidade Católica, 2012.

SILVEIRA, C.R.***Estudo de Formatos Especiais de Modulação Digital para Comunicações Ópticas.*** Dissertação de Mestrado. São Carlos: Universidade de São Paulo, 2009.

SOWAILEM, M. Y. S.; MORSY, M. H. S.; SHALABY, H. M. H. Employing Code Domain for Contention Resolution in Optical Burst Switched Networks With Detailed Performance Analysis . *Journal of Lightwave Technology*, vol. 27, no. 23, 2009.

SUCHAT, S.; PAIBOOD, S.; YUPAPIN, P. P. An Experiment of Optical Encryption Technique with Quantum Security for Mobile Phone Up-link Converter. *IEEE ICIT,* Bangkok,Thailand, 2002.

TAJAHUERCE, E.; MATOBA, O.; VERRAL, S.C.; JAVIDI, B. Optoeletronic information encryption with phase-shifting interferometry. *Applied Optics, Optical Society of America*, 2000, Vol. 39, nº 14, pp.2313-2320.

TANAKA, A.; FUJIWARA, M.; NAM, S. W.; NAMBU, Y.; TAKAHASHI, S.; MAEDA, W.; YOSHINO, K.; MIKI, S.; BAEK, B.; WANG, Z.; TAJIMA, A.; SASAKI M.; TOMITA, A. Ultrafast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Optical Express*, 2008. Vol. 16, pp. 11354-11360.

TOCNAYE, J.L.B.; CORNEJO, J.A. Implementation of a Noninvasive Data Encryption Technique Based on a Free-Space Spectral Phase Scrambling Scheme. *Optical Engineering*, vol. 47, nº 6, pp. 65004-1-65004-9, 2008.

TOWNSEND, P. Quantum Cryptografhy in Optical Fiber Networks. *BT Laboratories*, United Kingdom, 1998.

VIEIRA, M.A.M.; COELHO JR., C.N.; SILVA JR., D.C.; MATA, J.M. Survey on Wireless Sensor Network Devices. ETFA, Emerging Technologies and Factoring Automation, *IEEE Conference*, vol. 1, pp. 537-544l, 2003.

WANG, X.; WADA N. Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application. *Optics Express*, vol. 15, pp. 7319-7326, 2007.

WANG, X.; WADA, N.; HAMANAKA, T.; MIYAZAKI, T.; CINCOTTI, G.; KITAYAMA, K. I. OCDMA over WDM Transmission. *Transparent Optical Networks,* pp. 110 -113, 2007.

YIN, H.; RICHARDSON, D. J. Optical Code Division Multiple Access Communication Networks – Theory and Applications. *Tsinghua University Press and Springer-Verlag*, 2007. 382 p.

YONENAGA, K.; KUWANO, S. Dispersion-Tolerant Optical Transmission System using Doubinary Transmiter and Binary Receiver. Journal of Lightwave Technology, vol. 15, pp. 1530-1537, 1997.